(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－36049
（P2000－36049A）
(43)公開日　平成12年２月２日(2000.2.2)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６５Ｐ	
Ｇ０６Ｆ　19/00		Ｇ０９Ｃ　1/00	６４０Ｄ	
Ｇ０９Ｃ　1/00	６４０		６４０Ｂ	
5/00		5/00		
		Ｇ０６Ｆ　15/30	Ｈ	

審査請求　未請求　請求項の数１　ＯＬ　外国語出願　（全 69 頁）

(21)出願番号　特願平11－106565

(22)出願日　平成11年４月14日(1999.4.14)

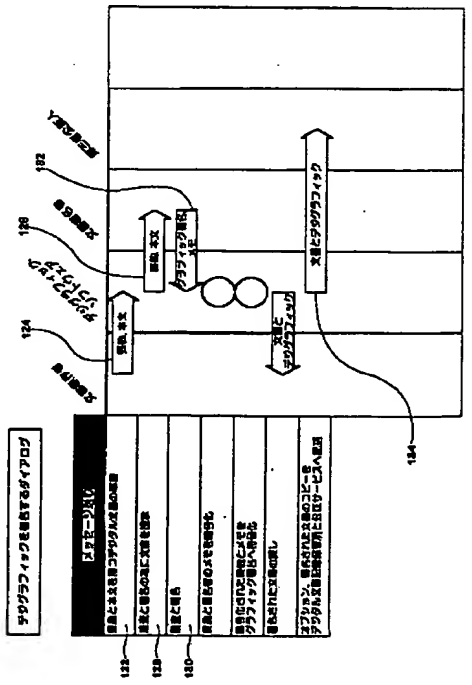
(31)優先権主張番号　６０／０８１７４８
(32)優先日　平成10年４月14日(1998.4.14)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／１９０７２７
(32)優先日　平成10年11月12日(1998.11.12)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／１９０９９３
(32)優先日　平成10年11月12日(1998.11.12)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　598156527
シティコープ　デヴェロップメント　センター，インコーポレイテッド
Ｃｉｔｉｃｏｒｐ　Ｄｅｖｅｌｏｐｍｅｎｔ　Ｃｅｎｔｅｒ，Ｉｎｃ．
アメリカ合衆国　カリフォルニア州　90066，ロスアンジェルス，ダヴリュー．ジェファーソン　ブールバード　12731
(74)代理人　100092956
弁理士　古谷　栄男　（外３名）

最終頁に続く

(54)【発明の名称】　デジタルグラフィック署名システム

(57)【要約】　（修正有）
【課題】各個人が電子文書上の自己署名を認知できるようにすると共に、署名しようとする文書を理解させ、後日、その文書の作成を想い出すことのできる、デジタルグラフィック署名システムを提供する。
【解決手段】システムは、作成される文書に関する情報を含む文書部分と、署名部分とを含み、ともに暗号化することができ、個人にとって容易に識別可能な単一オブジェクトへ併合することができる。用語「デジタルグラフィック署名」または「デジグラフィック署名」は、ここでは、併合されたオブジェクトを説明するのに利用される。本発明のデジタルグラフィック署名システムは、インターネット上およびネットワークシステム上での取引を含む電子取引で有利に利用することができ、また、情報バンキングおよびバーチャルワレットと併せて有利に利用することができる。また、私信の送信用のデジタルグラフィック印鑑も開示されている。



【特許請求の範囲】

【請求項１】複数のポイントを備える視覚的表現を持ち、個人がかかわる取引のための、デジタルグラフィック署名であって：取引詳細データに対応する少なくとも第１のカラーの併合されたポイントと、前記個人の署名データに対応する少なくとも第２のカラーのポイントとを含み、前記少なくとも第２のカラーポイントが前記個人の署名の視覚的表現を形成するようにした、デジタルグラフィック署名。

【請求項２】前記取引詳細データが：作成される前記文書の要約；作成される前記文書の本文；作成される前記文書の前記本文からの抜粋；または、
作成される前記文書に関する個人の注意書き；のうちの少なくとも１つを含む、請求項１のデジタルグラフィック署名。

【請求項３】前記取引詳細データが前記要約を含む、請求項２のデジタルグラフィック署名。

【請求項４】前記要約が、前記文書の作成により前記個人が実際に合意する対象の摘要を含む、請求項３のデジタルグラフィック署名。

【請求項５】前記要約が、以下のタイプの参照情報、つまり日付、関係当事者、または取引参照番号のうちのうちの少なくともひとつを含む、請求項３のデジタルグラフィック署名。

【請求項６】前記要約がテキストである、請求項３のデジタルグラフィック署名。

【請求項７】前記取引詳細データが、作成される前記文書の前記本文からの抜粋を含む、請求項２のデジタルグラフィック署名。

【請求項８】前記取引詳細データが、作成される前記文書の前記本文からの抜粋を備える、請求項３のデジタルグラフィック署名。

【請求項９】前記抜粋がテキスト形式である、請求項７のデジタルグラフィック署名。

【請求項１０】前記取引詳細データが、作成される前記文書の前記本文を含む、請求項２のデジタルグラフィック署名。

【請求項１１】前記取引詳細データが、更に、個人の注意書きを含む、請求項２のデジタルグラフィック署名。

【請求項１２】前記個人の注意書きが、前記取引の目的、前記取引の内容、または、前記個人にとり重要な他の詳細を含む、請求項１１のデジタルグラフィック署名。

【請求項１３】前記取引詳細データが、更に、個人の注意書きを含む、請求項３のデジタルグラフィック署名。

【請求項１４】前記個人の署名データが、前記個人署名のグラフィックから生成されるグラフィックデータを含む、請求項１のデジタルグラフィック署名。

【請求項１５】前記取引詳細データ、および前記個人の署名データが暗号化される、請求項１のデジタルグラフィック署名。

【請求項１６】前記併合されたポイントがカラー符号化される、請求項１のデジタルグラフィック署名。

【請求項１７】前記取引詳細データ、および前記個人の署名データがカラー符号化されており、前記要約はブルー値を含み、前記個人の注意書きはグリーン値を含み、前記個人署名データはレッド値を含む、請求項１３のデジタルグラフィック署名。

【請求項１８】前記視覚的表現が、ビデオ画面端末上に表示されることができる、請求項１のデジタルグラフィック署名。

【請求項１９】更に、前記複数のカラーのうち少なくとも１つで符号化されるデジタルグラフィック印鑑を含む、請求項１のデジタルグラフィック署名。

【請求項２０】デジタルグラフィック署名システムであって：前記請求項１のデジタルグラフィック署名；前記取引の詳細データのための入力装置；前記署名データのための入力装置；および、ビデオ画面端末；を備えるデジタルグラフィック署名システム。

【請求項２１】個人が作成する文書に対応するデジタルグラフィック署名を生成する方法であって：前記文書の要約を形成するステップ；前記個人署名を得るステップ；前記要約から文書要約データストリームを生成するステップ；前記署名から署名データストリームを生成するステップ；および、
前記文書要約データストリームと前記署名データストリームとを、デジタルグラフィック署名へ併合するステップ；を備えた方法。

【請求項２２】更に、
前記個人からメモデータを得るステップ；文書メモデータストリームを生成するステップ；前記文書要約データストリーム、前記文書メモデータストリーム、および前記署名データストリームを、デジタルグラフィック署名へ併合するステップ；を備えた、請求項２１の方法。

【請求項２３】個人が作成する文書に対応するデジタルグラフィック署名を生成する方法であって：前記文書に関する詳細を選定するステップ；前記文書の要約を形成するステップ；前記個人の署名を得るステップ；前記詳細から文書詳細データストリームを生成するステップ；前記要約から文書要約データストリームを生成するステップ；前記署名から署名データストリームを生成するステップ；および、
前記文書詳細データストリーム、前記文書要約データストリーム、および前記署名データストリームを、デジタルグラフィック署名へ併合するステップ；を備えた文書化方法。

【請求項２４】更に、
前記個人からメモデータを得るステップ；文書メモデータストリームを生成するステップ；および、
前記文書詳細データストリーム、前記文書要約データス

トリーム、前記文書メモデータストリーム、および前記署名データストリームを、デジタルグラフィック署名へ併合するステップ；を備えた、請求項２３の方法。

【発明の詳細な説明】

【０００１】

【関連出願とのクロスリファレンス】本出願は、開示が本明細書に引用されて組み込まれている、発明の名称が「バーチャルワレットシステム」である１９９８年４月１４日出願の米国特許仮出願第６０／０８１，７４８号を、米国特許法１１９条（ｅ）に基づき優先権主張する。本発明は、発明の名称が「バーチャルワレットシステム」である１９９８年１１月１２日出願の米国特許出願第０９／１９０，９９３号と、発明の名称が「情報バンキング」である１９９８年１１月１２日出願の米国特許出願第０９／１９０，７２７号とを、米国特許法１２０条に基づき優先権主張する。

【０００２】

【発明の分野】本発明は、電子商取引で使用するデジタルグラフィック署名システムに関する。このシステムは、作成される文書に関する情報を含む文書部分と署名部分を備える。文書部分と署名部分は暗号化され、個人が容易に識別できる単一オブジェクトに併合されてもよい。「デジタルグラフィック署名」、または「デジグラフィック署名」という用語は、本明細書では、併合されたオブジェクト(metged object)を説明するのに利用される。

【０００３】本発明のデジタルグラフィック署名システムは、インターネットおよびネットワークシステム上での取引を含めた電子取引で有利に利用されるであろう。本発明のデジタルグラフィック署名システムは、情報バンキングおよびバーチャルワレット(virtual wallets)と併せても、有利に利用されるであろう。

【０００４】本発明はまた、私信を送信するのに利用されることができるデジタルグラフィック印鑑に関する。

【０００５】

【発明の背景】現実社会(physical world)において、署名は、特にその所有者により容易に認知される。しかし、そのような物理的署名の正当性は検証するのが困難な場合がある。

【０００６】対照的に、デジタル社会(digital world)において、デジタル署名は、最新の公開キー暗号方式を用いて否認できない性質 (non-repudiation) をサポートするよう十分に検証可能である。しかし、そのようなデジタル署名は、人間にとって認知できる形にはなっていない場合がある。従って、個人が自らの署名を視覚的に認知できるようにするデジタル署名システムのニーズが存在する。この問題に加えて、電子商取引および電子金融取引 (electronic financial transaction) の世界では、解決を必要とする別の問題がいくつかある。

【０００７】第一の問題は、作成されるべきデジタル文書の内容に関する情報を、コンシューマへ提供することに関係する。この問題は次のように表すことができる、「呈示されている「文書」がデジタルである場合、コンシューマは自らが今何に署名しているかをどのようにして分かるのか？」更なる問題は、コンシューマ自身のデジタル署名とデジタル文書とを関連付けるコンシューマに関係する。この問題は次のように表すことができる、「デジタル文書に関連付ける自らのデジタル署名をコンシューマはどのように認知するのか？」コンシューマが、行った取引を忘れている場合に、電子および非電子商取引に従事する金融機関、販売店、業者、および／または、その他には問題が発生する。この状況は、一部は、取引と、取引を含む請求書をコンシューマが受取る間の時間的な長さによって生じるであろう。請求書に書かれた特定取引に関し追加の書類作成を請求するコンシューマから、多くのカスタマーサービス電話が寄せられることになる。多くの場合、コンシューマは誠意を持っているが、文字通りその取引を憶えていない。取引の内容と署名を示す文書を受取った上で、普通は、コンシューマが、その取引を思い出すか、またはその取引が不正であるかを認知できる。しかし、このプロセスは、要員、書類処理、および発送の能力を含むカスタマーサービス・インフラを維持することを含むので、機関にとってはコストがかかる。

【０００８】現実社会で現在抱える問題とコストが、電子取引の場ではもっと悪くならないとは限らない。多くの現行技術に伴う特定の問題は、文書または契約書を完成する署名の視覚的フィートバックがコンシューマに提供されないことにある。また、電子取引の請求時に提供されるデータが、コンシューマに対し、取引を思い出すのに十分なデータを提供していない可能性もある。

【０００９】上記、およびその他の問題は、本発明のシステムにより解決される。

【００１０】

【発明の概要】本発明は、各個人が電子文書上の自らの署名を認知できるシステムを提供するとともに、個人が署名しようとしている文書を理解させ、後日、その文書の作成を思い出すことをできるようにするであろう。文書関係情報を提供するシステムを提供する。

【００１１】本発明により、デジタルグラフィック（デジグラフィック）署名システムは、作成される文書に関する詳細と個人の署名とを組合わせることにより形成されるグラフィックを含む。文書の詳細と個人の署名は、従来技術を利用して暗号化され、セキュリティを高めることができる。デジタルグラフィック署名は、検査のためにユーザーインターフェースを介して表示することができる。

【００１２】デジグラフィック署名に組み込むことができる文書の詳細には：作成される文書の要約；作成される文書の本文；作成される文書の本文からの抜粋；また

は、作成される文書に関する個人のメモ；が含まれる。

【００１３】一般的に、文書を作成することによって、個人が実際に同意する対象の摘要を含む要約を少なくとも含めることが、多くの目的にとって有利であると信じられている。この要約には、日付、関係当事者、取引参照番号等を含めてもよいが、これらに限定はされない。要約は、比較的洗練されていないコンシューマでも容易に理解できる平易な（非法律的な）用語で書かれるのが好ましい。一般的に、要約は、デジグラフィック署名を形成する目的でテキストに短くされる。しかし、要約は、特定用途ではグラフィックつまり画像情報を含むことが有利な場合がある。

【００１４】特定の取引に対し、デジグラフィック署名に、要約に加えて、または要約の代わりに、作成される文書の本文、または作成される文書の本文からの抜粋、を含めることが有利な場合がある。文書本文および／または抜粋は、一般的に、デジグラフィック署名を形成する目的でテキストに短くされるであろう。しかし、特定用途に対しては、グラフィックつまり画像の情報を含むことが有利な場合がある。

【００１５】上述のように、文書の詳細は更に、個人のメモ領域を備えることができ、個人が、作成される文書について自己の選定した情報を記録できるようにする。将来、個人が取引を思い出すのを助ける情報を入力するのが好ましい。そのような情報は、取引の目的、取引の内容と同じく、個人にとり意味のある他の詳細を含めることができよう。

【００１６】個人の署名の表現は、個人の署名のグラフィックから生成されるグラフィックデータを含めてもよい。個人の署名グラフィックは、例えばグラフィックタブレットの使用を通じて、個人が名前を署名するために利用するペンストローク（ペンの動き）を取り込むことにより得られるであろう。また、個人の署名グラフィックは、物理的文書から署名をスキャンすることによっても得られる。一般的に、以下説明する変換と併合ステップを行う前は、個人の署名グラフィックは、物理的文書上の個人の署名に類似している。

【００１７】デジタルグラフィック署名を作成するには、文書の詳細データ個人署名データを併合する。併合プロセスは，従来の電子暗号化技術を利用する両セットのデータの暗号化を含んでもよい。文書の詳細を部分ごとに、公開キーまたは秘密キーを用いて暗号化することができる。

【００１８】例えば、従来の公開キー暗号方式技術を利用して、文書を作成する個人の秘密キーで文書要約データを暗号化することが有利である場合がある。次いで、要約は、個人にも、取引の他の当事者にもアクセスされ得るようにできよう。

【００１９】個人が入力するメモ・テキストデータは、個人だけが知る対称キーで暗号化されることもできよう。以下に説明されるように、これは、文書が偽造されていないという更なる保証を個人に提供し、取引を思い出す手助けを行うことができる。

【００２０】次いで、文書の詳細データと個人の署名データを、例えば、カラー符号化を利用して併合してもよい。この技術では、各データストリームは、例えば、標準ＲＧＢ（レッド、グリーン、ブルー）カラー符号化におけるカラー値として利用される。例えば、要約ストリームの各バイトを使って、ブルー値を生成してもよく、メモ・ストリームの各バイトを利用して、グリーン値を生成するようにしてもよい。変化しないレッド値を使って記述を完了するようにしてもよい。他のカラー値も利用することができる。例えば、ＣＭＹＫ（シアン 、マゼンタ、イエロー、黒）カラー符号化を利用して、データストリームに対応するシアン、マゼンダ、イエロー、黒、のカラー値によりデジタルグラフィック署名を作成することができる。

【００２１】デジタルグラフィック署名は、「カラーポイント」を使用する一連のインク・ストロークと、定義された署名領域に関する相対座標により定義されるポイントと、カラー値、として定義されてもよい。相対座標は、２次元署名領域における、Ｘ、Ｙ座標；ｒ、θ座標等や；または３次元署名領域における、Ｘ、Ｙ、Ｚ座標等を含んでいてよい。

【００２２】初期には、個人の署名データは、単一カラーの取り込まれたストロークを含んでいてよい。併合プロセス中に、初期カラー値は、符号化された暗号テキスト（cryptotext） 値に置換される。ポイント位置は、署名のグラフィック外見を保存するために保持されてもよい。

【００２３】署名データ、と要約および／またはメモ・ストリームデータとの長さ（バイト総数）の差は、双方向パディング（bidirectional padding）技術または、当該技術分野で通常に精通する者に理解される類似の技術で取扱うことができる。

【００２４】もし、署名データが、要約またはメモデータのいずれかより長ければ、ブルーおよびグリーン部分には、ゼロ値が用いられ、ゼロではなく、変化しないレッド値が、署名の残りのデータに使用されることができる。このようにして、要約および／またはメモデータが終了する場合であっても、署名のグラフィック外見が保存される。

【００２５】要約データおよび／またはメモデータが署名データより長い場合、ゼロポイント値がカラーポイントに割付けられる一方で、そのカラーが、残りのメッセージを符号化するのに使用される。残りのメッセージは、署名データのグラフィック表現と見做される必要はないが、デジタルグラフィック署名の一部として現われてもよい。

【００２６】結果として生じるデジタルグラフィック署

名は、個人の物理的な署名と類似する視覚的外見を有利に保持することができるが、しかし、レッド、グリーン、ブルーの各カラーのポイントを含むであろう。グリーンとブルーのポイントは特定の文書に特有のデータに対応して生成されるであろうから、レッド、グリーン、ブルーの各ポイントの相対量が、デジタルグラフィック署名を特定の文書に関連付けるであろう。

【００２７】当該技術分野で通常に精通する者には理解されるように、異なるカラー、つまり異なるカラー符号化方式は、本発明に従うデジタルグラフィック署名を生成する方法に類似する方法で利用してもよい。

【００２８】デジグラフィック署名は、例えば、＊．ｇｉｆ　ファイル；　＊．ｔｉｆｆファイル；　＊．ｐｉｃｔ　ファイル；　＊．ｊｐｇ　ファイル等のデータファイルとして保存され、取引用のデータファイルに関連付けられ、および／またはそこに蓄積されてもよい。デジタルグラフィック署名は、インターネットブラウザソフト、融取引ソフト、および／またはワープロソフト等の普及したコンピュータソフトウエアプログラムにより、ビデオモニターに表示されることのできるファイル形式で保存されるのが好ましい。

【００２９】従って、一局面では、本発明のデジタルグラフィック署名は、複数のポイントから生成される個人署名のグラフィック表現を含み、これら複数のポイントは、少なくとも、作成される文書に特定する情報に対応するポイントの第一のセットと、個人の署名に対応するポイントの第二のセットを含む。

【００３０】他の局面では、本発明のデジタルグラフィック署名は、ビデオモニターに表示できる個人の署名の視覚的に認知可能なマルチカラーグラフィック表現を含み、このグラフィック表現は、作成される文書に対応する単一カラー方式を有する。本明細書中で使われるように、用語であるビデオモニターは、コンピュータビデオモニター、テレビおよび類似品を含む。

【００３１】本発明によれば、デジタルグラフィック署名システムは、本発明のデジタルグラフィック署名と、デジタルグラフィック署名システムを生成し表示できるコンピュータのソフトウエアと、ハードウエアとを備える。コンピュータハードウエアは、中央演算処理装置、ビデオモニター・ディスプレイ；メモリ；モデム；キーボード；マウス；トラックパッド；グラフィックタブレット；スキャナ；プリンタ；および／またはその他一般的に利用できるコンピュータハードウエア・コンポーネントを備えていてもよい。コンピュータハードウエアは、グラフィックタブレット；電子ペン；タッチスクリーン；マウス；トラックボール；ジョイスティック；電子ペン（訳注：前に同じ記述あり）；ＰＯＳ電子ペン装置、または個人の署名を「ペンストローク」として取り込む同様な入力装置を含むことが一般的に好ましい。それと同一の入力装置、またはキーボードのような他の入力装置は、作成される文書に関するメモに対応するメモデータファイルを個人が作成できるようにするのの役立つ。

【００３２】本発明のシステムで役立つコンピュータソフトウエアは、データストリームおよびカラー符号化データストリームを暗号化するための暗号化ソフトウエアを含む。ワープロプログラム、グラフィックプログラム等の、追加ソフトウエアも、例えば、個人が取引に関するメモを入力できるようにするために、そしてデジタルグラフィック署名を見るために有用だろう。

【００３３】また、本発明は、個人が作成する文書に対応するデジタルグラフィック署名を生成する方法を提供し、その方法は：文書の要約を形成するステップ；個人の署名を得るステップ；要約から文書要約データストリームを生成するステップ；署名から署名データストリームを生成するステップ；および、文書要約データストリームと署名データストリームとを、デジタルグラフィック署名へ併合するステップ；を有する。

【００３４】その方法は、更に：個人からメモデータを得るステップ；文書メモデータストリームを生成するステップ；および文書要約データストリームと、文書メモデータストリームと、署名データストリームとを、デジタルグラフィック署名へ併合するステップ；を有していてもよい。

【００３５】代替実施形態において、本発明は、個人が作成する文書に対応するデジタルグラフィック署名を生成する方法を提供し、その文書化方法は：文書に関する詳細を選定するステップ；文書の要約を形成するステップ；個人の署名を得るステップ；詳細から文書詳細データストリームを生成するステップ；要約から文書要約データストリームを生成するステップ；署名から署名データストリームを生成するステップ；および、文書詳細データストリームと、文書要約データストリームと、署名データストリームとを、デジタルグラフィック署名へ併合するステップ；を有する。

【００３６】この方法は、更に：個人からメモデータを得るステップ；文書メモデータストリームを生成するステップ；文書詳細データストリームと、文書要約データストリームと、文書メモデータストリームと、前記署名データストリームとを、デジタルグラフィック署名へ併合するステップ；を有していてもよい。

【００３７】データストリームは、以上に上で説明し、以下詳細に説明する技術を利用して得られ、併合されてもよい。加えて、データストリームは暗号化されてもよい。

【００３８】更なる局面で、本発明は、例えば、取引する２当事者のような、２当事者間の私信を提供する方法と手段を提供する。本発明は、ここで「デジタルグラフィック印鑑」または「デジグラフィック印鑑」と呼ばれる機能を提供する。デジタルグラフィック印鑑は、本明

細書中で検討される本発明のデジタルグラフィック署名へ追加機能を提供してもよい。当該技術分野で通常に精通している者により理解されるであろうように、デジタルグラフィック印鑑は、独立して利用されてもよい。

【００３９】本明細書で検討するように、本発明のデジタルグラフィック署名、システム、および方法は、デジタル署名やデジタル証明書単独と比較して、向上させた機能を提供している。それらは、コンシューマがデジタル文書に署名するのに安堵感を覚え、かつ署名したデジタル文書を認知できるという知覚ニーズを解決する一方、署名が偽造されなかったこと、そして署名が他の文書からコピーされたのではないという確信を抱かせる。

【００４０】本発明の署名、システム、および方法は、例えば、署名者が取引を思い出す際にそれを支援するメモを許容することによって、認知可能で、役に立つヒューコンファクターを、従来の暗号方式のに加える。更なる利点は、本発明によるデジタルグラフィック署名が、一般的に従来のデジタル証明書よりも小型で、それ故に、蓄積目的、およびネットワークのトラフィック負荷を減少させるため、より望ましいであろう。これらは、その内容が、最適な普及暗号方式技術を使いながらも、デジタル署名情報を含むと共に、手書き署名の認知可能なグラフィックを表現することを含むことができるという点で、デジタル署名の世界では無比である。

【００４１】本明細書で検討するように、本発明のデジタルグラフィック署名は、ステガノグラフィ（steganography）に類似する技術を利用して、グリーンカラー・バイトの署名者のメモ、およびブルーカラー・バイトの文書の要約を、それらの手書きの署名のグラフィック表現へと符号化してもよい。

【００４２】グラフィック内に存在し、符号化されているメッセージがあるという事実を隠すことは厳密には必要ではないので、この技術は、技術的にステガノグラフィであるとは限らない。従って、デジグラフィック署名は２者以上の当事者間の通信の内容を隠そうとは試みていない。メモは、署名者による使用だけを意図するのであって、署名者にだけ知られた機密キーを使用する。署名者の公開キーを持つ何れの第三者も、署名を検証できる。その目的は署名者の認証のためであり、そして不否認取引を保証するためであり、私信の暗号化のためではない。しかし、本発明のデジタルグラフィック署名を暗号化することは可能であり、そのような実施形態が本発明の適用範囲内に含まれることは、言うまでもない。本発明の実施形態の利点は、更なる暗号化が必要ではないことである。

【００４３】デジタルグラフィック「印鑑」という用語は、二当事者間の私信を封印するのに使用されていた、昔からの概念である印鑑付指輪からの借用である。しかし、この類比は、昔の世界では直ちに崩れ去り、破損した封印が示すことは、プライバシーが傷つけられてしまったということである。それは、プライバシーが傷つけられるのを防ぐことはできなかったのである。本発明によると、デジタルグラフィック印鑑は、更に２当事者間の機密の通信を含む、本発明のデジタルグラフィック署名の実施形態である。デジタルグラフィック印鑑は、カラー値、例えば、機密通信の符号化と送信のためにＲＧＢカラー方式でのレッドカラー値を利用する。更なる詳細を以下に述べる。

【００４４】本発明のデジタルグラフィック印鑑は、機密通信をデータストリームに符号化することによる、本発明の方法で利用されることができる。

【００４５】本発明のデジタルグラフィック署名、デジタルグラフィック印鑑、システム、および方法は、インターネットおよびネットワークシステム上での取引を含む、電子取引で有利に利用されてもよい。本発明のデジタルグラフィック署名システムは、発明の名称を「バーチャルワレットシステム」とする１９９８年１１月１２日出願の米国特許出願第０９／１９０，９９３号；発明の名称を「情報バンキング」とする１９９８年１１月１２日出願の米国特許出願第０９／１９０，７２７号；関連技術で、発明の名称を「電子的データを安全に蓄積するシステムおよび方法」とする１９９９年４月＃＃日出願の米国特許出願第０９／＃＃＃，＃＃＃号；および、発明の名称を「インターネットウエブサイトへの蓄積情報伝送を制御するシステムおよび方法」とする１９９９年４月＃＃日出願の米国特許出願第０９／＃＃＃，＃＃＃号；等に記載の情報バンキングおよびバーチャルワレットに関連して有利に利用されることができる。これら各出願の開示は、本明細書中に引用して組み込む。

【００４６】本発明のデジタルグラフィック署名システムおよび方法の利点は、以下を含む。

【００４７】個人は、自己の署名を視覚的に認知できる。

【００４８】先の代替実施形態では、グラフィックを、個人の署名文書とともに含めることができよう。しかし、伝統的なグラフィックは容易にコピーされ、それ故、偽造するのが比較的簡単である。加えて、グラフィックと作成される文書とを確実に関連付けるという特性は伝統的なグラフィックには全くない。対照的に、本発明を利用して作成されるデジタルグラフィック署名は、偽造するのが相対的に困難で、作成される文書に関連付けられる。

【００４９】更なる利点は、本発明のデジタルグラフィック署名が検証され得ることである。個人が本当に文書を作成した者であったかを検証するには、公になった公開キーが、署名の要約部分を復号化するのに利用されることができるだろう。本発明に従えば、この要約はグラフィック署名へと符号化される。要約は、文書内で暗号化されていない文書の要約と厳密に一致しなければならない。これは、（コンシューマは署名を生成した秘密キ

一を所有している唯一の者であるから）文書がそのコンシューマにより署名されたことを証明するとともに、要約一致に起因して、不自然さが特定の文書に関連付けられるということを証明する。

【００５０】加えて、個人は、自らの機密キーを使用して、グラフィック署名に符号化されたメモを読むことができる。メモが、文書中に無くて他人には復号化され得ない限り、要約とは違って、メモは、文書が偽造されなかったという更なる保証を個人に提供する。メモはまた、個人が文書を思い出すのを支援することもできる。

【００５１】本発明のデジタルグラフィック印鑑の実施形態の利点は、デジタルグラフィック署名が、２当事者間の機密通信を含み得ることにある。

【００５２】本発明の更なる詳細と利点は、以下の記述および添付図面から明らかになるであろう。

【００５３】

【発明の詳細説明】本発明のデジタルグラフィック署名システムおよび方法の特徴と利点は、図面を参照して以下の段落で説明される。

【００５４】図１は、本発明による、個人「John Doe」のデジタルグラフィック署名の可能性のある実施形態を示す。図１に示すように、本発明のデジタルグラフィック署名は、個人の手書き署名に類似する視覚的外見２を有する。断面図に示すように、視覚的表現は、複数の異なるカラー内の個別ポイントにより形成されている。例えば、視覚的表現は、グリーンポイント４、ブルーポイント８、レッドポイント６により形成されていてもよい。各カラーのポイントの相対数および位置は、各取引にとって一義的であり、デジタルグラフィック署名を生成するためカラー符号化される文書データおよび署名データの相対的な量と種類をベースにしているであろう。しかし、一般的に、全体の視覚的表現は、個人の手書き署名に類似していて、認証を簡素化するであろう。

【００５５】デジグラフィック署名の簡単な実施形態は、グラフィカル・ユーザーインターフェース（ＧＵＩまたは単にＵＩ）を含み、ユーザーが以下を見ることを可能にする：

１）　署名される文書の要約
２）　署名される文書の本文または詳細
３）　名前をグラフィックに署名する署名パッド領域
４）　パーソナルメモの領域

要約は、文書に署名することによりコンシューマが実際に合意する対象の摘要を含んでいてもよい。要約は、平易な（非法律的な）用語であり、テキスト表現にまで短く（欠けたテキストまたはグラフィック等）されている。事実上、要約は実際に署名されるものである。要約は、例えば、契約の日付および当事者の名前を含む関連した他の事項を追加で含んでいてもよい。

【００５６】一旦コンシューマが文書を読み、署名する決心をすると、署名領域へ移行し、名前をグラフィックに署名する。更に、コンシューマは、作成している取引を思い出すよう、パーソナルメモ領域へメモを入力するよう推奨されてもよい。

【００５７】文書へ署名するのに利用されるペンストローク、およびメモは、コンピュータシステムのハードウエアおよびソフトウエアを経由して取り込まれる。加えて、コンピュータシステムは、要約とメモのテキストをグラフィック署名へと符号化するであろう。好ましい技術はステガノグラフィに類似する。

【００５８】最初、２つのメッセージストリームは、モデム暗号方式を使用し暗号化される。要約は、モデムの公開キー暗号方式技術を使用し、コンシューマの秘密キーで暗号化されてもよい。メモテキストは、コンシューマだけが知る対称キーを使用して暗号化されることができる。

【００５９】２つの暗号化されたストリームは、次いで、標準の、レッド、グリーン、ブルー（ＲＧＢ）カラー符号化でカラー値として使用される。例えば、要約ストリームの各バイトは、ブルー値の代わりに用いられ、メモストリームのバイト値は、グリーン値を要求する。変化しないレッド値は、記述を完了するのに使用されるであろう。

【００６０】グラフィック署名は、「カラーポイント」を使用する一連のインク・ストローク、（定められた署名領域に関するｘ－ｙ相対座標に対応する）ポイント、およびカラー値として定義される。取り込まれるインク・ストロークは、最初は単一カラーで取り込まれる。符号化プロセス中に、カラー値は、符号化された暗号テキスト値に置き換えられる。ポイントの位置は、勿論、署名のグラフィック外見を保存するように保持される。

【００６１】グラフィック署名ストロークと、要約およびメモストリームの長さ（バイト総数）における差は、双方向パッディングにより処理される。もし、グラフィック署名が２つのメッセージのいずれかより長ければ、ゼロ値がブルーとグリーンの部分に用いられ、唯一ゼロでない、変化しないレッド値が用いられる。このようにして、署名のグラフィック外見は、メッセージが終了する場合でも保存される。もし、メッセージのうちのひとつがグラフィック署名より長ければ、ゼロポイント値は、カラーポイントに割付けられる一方で、そのカラーがそのままメッセージの残りを符号化するのに使用される。インターフェースは、位置の値を持たないストロークを引出さないように設計されるが、署名の引出されない部分は、依然としてメッセージを保存する。

【００６２】ユーザー署名のグラフィック表現は、デジタル署名と共に単一オブジェクトへと既に併合されている。この併合されたオブジェクトは、いくつかの利点を有し、以下を含む。

【００６３】コンシューマは、自己の署名を視覚的に認知できる。先の代替実施形態では、グラフィックは、コ

ンシューマの署名の文書に含められるかもしれない。しかし、通常のグラフィックは容易にコピーされ、それ故に偽造される。加えて、文書と確実に関連付く、という特質は従来のグラフィックにはない。

【００６４】コンシューマが本当に文書に署名した人であったかを検証するには、コンシューマの公開キーが利用されて、署名の要約部分を復号化することができる。デジタルで署名された要約は、グラフィック署名へと符号化される。加えて、要約は、文書内で「明文である」（in the clear）か、または暗号化されていない文書の要約と厳密に一致しなければならない。この一致は、１）署名はコンシューマにより署名されたこと（何故なら、コンシューマが署名を作った秘密キーを所有している唯一の人である）そして、２）署名が、要約の一致により特定の文書に関連付くこと、を証明する。

【００６５】加えて、コンシューマは機密キーを使用してグラフィック署名へと符号化されたメモを読むことができる。メモが文書中に無く、他人により復号化され得ないため要約とは異なり、メモは、文書が偽造されなかったことをコンシューマへ更に保証し、また、取引を思い出すのを助ける。

【００６６】図２は、デジタルグラフィック（デジグラフィック）署名を生成するプロセスの概略図を提供する。図２に示すように、本発明に従うデジグラフィック署名プロセスの実施形態は、文書の要約１０２を含み、それは秘密キー１０４を使用して、非対称暗号化エンジン１０３において暗号化されている。プロセスは、更に、機密メモ１０６を含むことができ、それは機密対称キー１０８を使用して、対称暗号化エンジン１０７において暗号化されている。次いで、暗号化された要約および／または暗号化されたメモは、署名パッド上での個人の署名により生成されるグラフィック署名インク・ストローク（カラーポイントの整列集合）１１０を用いて符号化されることができる。

【００６７】２つの暗号化されたストリームは、上述のように、標準のＲＧＢカラー符号化でのカラー値として使用される。図２で、暗号化された要約バイト１１１は、ブルーに対応し、暗号化されたメモバイト１１３は、グリーンに対応する。グラフィック署名は、上述の方式では、カラーポイント１１２を使用する一連のインク・ストロークとして定義される。結果として得られるオブジェクトは、個人の署名とデジタル署名との単一のオブジェクト１１４への併合を含む。

【００６８】図３は、デジグラフィック署名ダイアログの概略フローチャートを示す。フローチャートに示されるメッセージ送りはソフトウエアで作成され、デジグラフィック署名機能を使用する者からの入力に対応するであろう。図３に示すように、初期ステップ、つまりメッセージ送りは、デジタル文書を要約と本文とともに準備するステップである（１２２）。このステップで、文書作成ソフトウエアは、文書の本文および要約をデジグラフィックソフトウエアへ転送、または入力する（１２４）。次いで、文書は、デジグラフィックソフトウエアにより読まれ、ソフトウエアが、文書要約と文書本文を生成する（１２６）。文書要約の Ted Smythe 用のサンプルが図４に示され、文書本文のサンプルは図５に示されている。

【００６９】図４に示すように、文書要約２００は、Windows Ｒ画面２０４で作成される文書に関する詳細２０２を含むことができ、画面はタブ２２１（「要約」）、２２２（「本文」）、２２３（「署名」）を含む。「要約」タブの下に、文書要約２００は、取引に関する事実の詳細を含むことができ、図４に示す以下の詳細を含むが、これらに限定はされない：

【００７０】

日付	０３／２３／１９９８
請求書	３５２８６４
小売店	Radioshack ０１－３５１６
販売先	Ted Smythe
クレジットカード種類	Ｖｉｓａ
口座番号	４３２１－２３４５－６７８９－３４５６
有効期限	０４／９９
取引番号	１４８５
承認	０２３５９８
注：	カード発行者が表示合計金額を負担
条件	販売と返品は合意の条件と規約による
謝辞	Radioshackでのお買上げありがとうございます
請求金額	２７．５１

【００７１】図５は、その要約が図４に示されている取引のサンプルに対する文書本文のサンプル２１０を示す。図５に示すように、文書本文は、Windows Ｒ画面２１４で作成される文書の文書本文のテキスト詳細２１２を含むことができ、画面はタブ２２１（「要約」）、２２２（「本文」）、２２３（「署名」）を含む。文書本文２１２は、「本文」タブの下に表示されてもよい。

【００７２】図３に戻り参照すると、文書に署名する人

は、文書要約と本文を検討（１２８）し、文書を思い出すのに役立つメモを入力するよう指示され、その後に署名が続く（１３０）。図６は、メモと署名を指示するユーザーインターフェースの可能な実施形態を示す。

【００７３】図６に示すように、署名ユーザーインターフェース２２０は、Windows®画面２２４で作成することができ、画面はタブ２２１（「要約」）、２２２（「本文」）、２２３（「署名」）を含む。「署名」タブの下に、署名ユーザーインターフェース２２０は、メモ領域２２６、グラフィック署名領域２２８、および個人が作成する文書に関しパーソナルメモを入力できるメモ入力領域２３０、を含んでもよい。メモ入力領域２３０は、初期には、ユーザーにパーソナルメモを入力することを指示するテキスト・プロンプトを含んでもよい。インターフェース２２０は、更に、ボタン２５１（「署名」）、２５２（「認証する」）、２５３（「送信する」）を含んでもよく、これらは、ユーザーが署名して、その署名を確認して送信することを可能にする作成ルーチンにリンクされている。

【００７４】署名後、ユーザーにより入力されたプライベートメモ、および文書要約は、ユーザー署名へと符号化されたデジグラフィック署名へ戻される（１３２）。図７は、ユーザー「Ted Smythe」の符号化されたグラフィック署名１４０の可能な実施形態を図示する。次いで、ユーザーは、例えばウインドウ２３０においてテキスト・プロンプトに指示されて、ユーザーと文書原作者の間の取引を完了させる。文書に「署名」するよう符号化されたグラフィック署名を文書原作者へ送信し、図３の１３４に示すように、署名された文書およびデジタルグラフィック署名は、オプションとして、デジタル署名を検証する為にデジタル文書アーカイブまたは公証サービスへ配信されてもよい。公証サービスは、署名者の公開キーを利用して、署名が偽造されなかったことを検証するであろう。

【００７５】本発明のデジタルグラフィック署名システムは、１９９８年１１月１２日出願の米国特許出願第０９／１９０，９９３号に記載されているシステムのような、バーチャルワレットシステムで有利に利用することができる。

【００７６】バーチャルワレットでは、ワレット所有者の署名は、所有者により認知されることができる書式で、請求書または受領書へ有利に添付してもよい。本発明の最終的な署名済み文書の書式は、デジタル署名を人が認知できるようにすることにより、典型的なデジタル署名を凌駕するものである。最終的な署名済み文書の書式は、署名が自己のものであると視覚的に判別し、署名と特定の文書を関連付け、署名と文書が偽造されていない、あるいはコピーされていないことを、所有者が検証できるようにする。署名は、本発明のデジグラフィック署名を含むとともに、ワレット所有者が自己のものであると認知できるグラフィックおよびデジタル署名を含む。電子文書中に認知可能で、判定可能なデジタル署名を提供するという特徴は無比のものであり、ワレット所有者が自己の手書き署名を紙の文書で認知するのに類似している。この特徴は、ワレット所有者が特定の取引を思い出し、自己の署名を検証する手助けをする。デジタルグラフィック署名に関する更なる詳細は上記の通りである。

【００７７】書式とは係わりなく、署名される必要のある文書に対し、文書は少なくとも要約および本文を備えていることが推奨される。明文の要約としても知られる要約は、平易なグラフィックでないテキストで呈示される文書に署名する場合にコンシューマが合意したことの摘要を含む。要約は、取引の、支払い、配送、または条件と規約に関する情報、または他の同様な情報であってもよい。例えば、要約での支払い情報は、日付、関係当事者、取引の一般的な内容、および支払い金額を含んでいてもよい。本文は、文書として通常参照される書式の情報を全て含む。従って、本文は、取引に関連付けられた詳細の全てを含む。一旦文書が署名されれば、それは少なくとも３つの要素、すなわち、要約、本文、および署名を持つ。しかし、一般的な条件と規約部分、出荷情報等のような他の要素があってもよい。そのため、この書式情報を適切なイネーブルブラウザへ送ることにより、例えば、請求書がワレット所有者に提出され得る。

【００７８】操作においては、図３を参照すると、レストラン等の署名要求者は、ワレット所有者に受領書等の文書に署名することを求める。要求者は、ダイアログを開始し、文書と要約を送る。本発明の特徴は、特に文書と要約を書式化し、ソフトウエアによる認知のための署名文書として指定する。ワレットサーバーは、オンライン状態になると、署名文書をワレットインターフェースへ送り、それによって、同期および非同期の両ダイアログをサポートする。ワレットインターフェースは、署名を行うための署名文書と要約とを、ワレット所有者に対して表示する。次いで、所有者は、署名のキーニックネーム(key nickname)のうちからひとつをピックアップする、すなわち換言すれば、キーニックネームを使って署名している人物をピックアップし、文書へグラフィック的に署名する。チップデバイスは、秘密キーを用いて要約を、機密キーを用いて暗号化する。このことは、秘密キーに見合う公開キーを持つ者は誰でも文書にアクセスするのを可能にする一方で、所有者に対して、そして公開キーであってもなくてもよい機密キーへのアクセス権を与えられた他の者に対して、メモは機密に保たれる。今や、署名済み文書は、本文、要約、およびデジグラフィック署名（ＤＳ）を含む。ＤＳは、要約が秘密キーで暗号化されたことにより、デジタル署名を含む。

【００７９】更に、チップデバイスは、署名済み文書と、関連付けられたインデックスとをワレットサーバー

へ戻す。チップデバイスは、インデックスを記憶するタスクを割当てられているので、ワレット所有者はその点を心配する必要がない。ワレット所有者はオフライン状態であってもよい。ワレットサーバーは、署名済み文書をアーカイブし、インデックス、文書のＩＤ、および署名の保証人のＵＲＬを、この情報を蓄積する署名要求者へ転送する。最後に、要求者は情報の受領を確認する。このように、本発明のこの特徴は、多数の署名キーおよび関連インデックスを有利に管理する。

【００８０】本明細書で説明されるように、好ましいデジグラフィック署名が文書への署名使用される場合、デジグラフィック署名オブジェクトは、要求されたときに署名のグラフィックをどのように描写する化を認識する。デジグラフィック署名はまた、デジタル署名を含んでいる。デジグラフィック署名は、第三者が署名の検証を実行するための行動様式、および文書署名者が自己の署名を検証して文書への関連の有効性を検証するための行動様式を内蔵している。更に、当該技術に精通する者が以下の記述から理解するように、好ましいデジグラフィック署名は、文書の認証と認定に有利に役立ち、かさばるデジタル証明書の必要性をなくす。

【００８１】図８は、文書に署名した個人（署名者）が、実際に文書へ署名したか確信が無いときに用いることができる、または、取引を記憶していなくて暗号化されたメモを検分することを望むときに用いることができる文書認証を説明するフローチャートである。文書の読出しにおいて、署名者は、文書上の署名１４０を検分することができる。可能性のある実施形態は、図９においてインターフェース２２０で示される。ユーザーは、例えば、図９のウインドウ２３０において署名の検証１５０（図８）を要求するよう指示されてもよい。検証を要求することにより、可能性のある署名者の（検証者の）機密キー１５２が、署名に付随するメモの復号化に利用される（１５３）。機密キーを使用するために、ユーザーは、パスワードを入力するよう指示されるであろう。可能性のある署名者の公開キー１５４が、署名と文書要約を復号化するのに利用される（１５５）。復号化されたメモと文書要約は、次いで、実際のメモと文書要約と比較され（１５７）、それらが一致するかどうかが、署名者へ、例えば図９のウインドウ２２８および２３０に表示されて、文書に署名したことを署名者が確認できるようにする（１５９）。可能な実施形態が図１０に示されている。

【００８２】図１０に示すように、署名１４０（"Ted Smythe"）は、ウインドウ２２８に、パーソナルメモはウインドウ２２６に、および文書要約はウインドウ２３０に表示され得る。図１０では、文書要約は、図４に図示された要約に一致する。

【００８３】もし、メモ、要約、および／または署名が復号化できない、または文書のものと一致しないと、ユーザーに警告メッセージが表示され、署名者が文書原作者へ偽造の可能性を通告することができる（１６１）。

【００８４】本発明の他の特徴は、図８を参照すると、自らのデジタル署名を認知したいコンシューマの気持ちを更に有利に解決する。ワレット所有者が署名した文書上の署名の正当性を検証することを望むとき、ローカル検証機能が利用される。代替または追加として、システムは、文書が開かれる都度に署名を自動的に検証し、不一致があったときはその都度ワレット所有者に警報だけを発するようにしてもよい。例えば、警告は「署名が要約と一致しない」と、いうように述べてもよい。

【００８５】この場合、ワレット所有者は、文書と要約を文書アーカイブから検索し、文書アーカイブは、所有者のパソコン上、ワレットサーバー内、または、その他の類似装置内に常駐していてもよい。先に検討したように、文書は、デジグラフィック署名を利用して署名されるのが好ましい。ワレット所有者は、例えば署名が偽造されていないことを確認することを望み、検証を要求する。ワレットインターフェースは、公開キー・リクエストを安全なチップデバイスへ送り、デバイスは文書に関連して以前に蓄積されたキーを戻す。次いで、インターフェースは、そのキーを使用して、要約を含む署名のデジタル部分を復号化する。インターフェースは、復号化された要約情報を、明文の要約情報、または文書中で暗号化されていない要約と比較する。この比較は、署名が所有者により署名されたことを証明する、何故なら、所有者は署名を作成した秘密キーを所有する唯一人であるからであり、要約の一致により、署名が特定文書に関連付けられていることを証明する。更に、署名のグラフィック部分は、所有者に認知可能であり、グラフィック署名と併合された要約の復号化が、明文の要約と一致する事実は、所有者にその正当性を保証する。このように、次いで、ワレットインターフェースは、検証チェックの結果を報告するメッセージを、所有者が検分するよう送り返す。

【００８６】デジタルおよびグラフィックの比較の組合せは、署名が特定文書に対して検証されることを有利に可能にする。この特徴は無比であり、検知されずにコピーされるかもしれないビットを含むデジタル署名を単にチェックするのに比較して、高度の信頼性を与える。このように、この特徴は、デジグラフィック署名がオリジナルの署名であり、単にオリジナルのように見えるものではないことを検証する。

【００８７】加えて、この特徴は、有利なことに、ワレット所有者だけにメモの復号化を許可し、そのメモは、文書内で他の場所には保存されていない、ワレット所有者に取引を思い出させるものを含むことができる。

【００８８】図１１は、本発明のデジグラフィック署名システムで使用される、可能な公開署名検証ダイアログのフローチャートである。このダイアログは、例えば、

販売点または公証人のような署名者でない者が、署名の検証を希望するときに使用することができる。上述のように、署名者だけが、署名に関連するメモテキストを検分することができる。更に、要求当事者が保持する文書およびデジタルグラフィック署名と、第三者の公証人ののそれとの比較オプションは、図１１には含まれてはいないが、そのような特徴を同様のステップにより加えてもよい。

【００８９】図１１に示すように、デジタルグラフィック署名の検証のためのリクエストが、第三者の要求者により行われる場合（１７１）、署名者の公開キー１５４が、文書の復号化に利用される。この公開キーは、前もって要求者に供給されているであろう。公開キーは、文書要約を復号化する（１７３）。復号化された要約は、実際の文書要約と比較され（１７５）、その結果、または一致しない場合の警告が、要求者へ表示される（１７７）。

【００９０】図１１を参照すると、本発明は、電子署名検証のために、電子メール、ダイレクトログイン、またはWWWを通したサービスを提供する。この場合、検証要求者は、署名済み文書、文書ＩＤ、および署名者のインデックスを署名保証人へ送る。例えば、WWW上では、このように見えるであろう：

http://www.citibank.com/verifysignature
署名：　（デジグラフィック署名を挿入）
署名者：　（インデックスを挿入）
対象：　（文書ＩＤを挿入）
添付：　（要約を挿入）

【００９１】署名者のインデックスは、署名の各保証人に対して一義的であるため、誰が署名者で、何の公開キーが使用されたか、は知られている。また、文書ＩＤは、ワレットサーバー内で見付けられるようにしてもよく、サーバーは、文書が最初に署名されたときに少なくとも文書の要約をアーカイブしている。最終的に、要約は、検証要求者が署名の検証を作成するよう求める文書である。

【００９２】署名保証人は、公開キーアーカイブ内の公開キーをルックアップするのにインデックスを利用する。次に、署名保証人は、公開キーを使用して、検証される署名を復号化する。署名がすべて復号化すると、それは、署名が署名者の記録に由来することを検証する。文書ＩＤを使用することにより、署名保証人は、要約のコピーをルックアップして提示された要約と比較し、それが正しい文書上の正しい署名であることを更に検証する。次いで、署名保証人は結果を検証要求者へ戻す。

【００９３】本発明のこの特徴は、インデックスと文書ＩＤを有利に利用して、その署名を検証する。他方、現行方法では、公開キー、証明書の証明者、および要約等、大量の情報を含む証明書を必要とする。更に、この大量の情報故に、現行方法を使用する署名保証人は、プロセスを保証する際に積極的な役割を持たない。これに対し、署名保証人は、本発明では非常に積極的な役割を持つ。このように、本発明のこの特徴は、署名の検証をより効率的に、かつより経済的に可能にする。

【００９４】先の説明から分かるように、本発明のデジタルグラフィック署名システムは、多くの有利な特徴を含んでいる。

【００９５】本発明に従えば、デジタル署名および機密のメモは、単一のグラフィック署名へ有利に符号化されることができる。

【００９６】更なる利点は、グラフィック署名を、文書の署名者が認知できることであり、署名者はまた、署名が特定の文書に関連付けられており、署名者により実際に署名されて、偽造されていないことが保証される。

【００９７】本発明のデジタルグラフィック署名システムの更なる利点は、署名のデジタル部分が、署名者のセキュリティキーの公開部分の知識を持つ第三者により検証することができることである。

【００９８】本発明のデジタルグラフィック署名システムのより更なる利点は、文書に関連付けられたメモを、文書の署名者の機密にとどませることである。

【００９９】本発明のバーチャルワレットシステムの説明にあるように、本発明のデジタルグラフィック署名システムは、本発明のバーチャルワレットシステムと併せて有利に利用することができる。

【０１００】図１２は、デジタルグラフィック印鑑を含む、本発明のデジタルグラフィック署名システムの概略図を示す。暗号化された要約バイト１１１および暗号化されたメモバイト１１３は、上記および図２に示すように生成される。オフページ接続子(off page connector)「Ａ」は、先の検討で、前にそれが行ったように符号化プロセスへ入るストリームを表す。同様に、機密メモは前と同じ方法で符号化される。オフページ接続子「Ｍ」は、前に行ったように符号化プロセスへ入るストリームを表す。

【０１０１】図１２に示す本発明のデジタルグラフィック印鑑の実施形態では、レッドカラー・バイト値３０２は私信に利用される。図１２に示すように、私信３０４は、テキスト表現に短くすることができ、送り主（署名者）の秘密キー３０６を使用して暗号化され得る。暗号化の結果３０８は、次いで、受取人の公開キー３１０を用いて再度暗号化される。引き続き、最後の操作の結果は、デジタルグラフィック署名に関し図２を参照した先の検討で説明されたカラーポイントオブジェクトストリーム内のレッドカラー値として、バイト毎に使用することができる。

【０１０２】通信の受取りにより、受取人は、最初にその秘密キーを使用して、第一層を復号化するであろう。デジタルグラフィック署名とは異なる文書付きのデジタルグラフィック印鑑を受取ることになるため、レッドカ

ラー値には私信があることを知り、デジタルグラフィック署名とは異る処理を行うであろう。第一層を復号化すれば、送り主の公開キーを使用して、最終層を復号化するするであろう。二重暗号化および暗号化と復号化の順序は、いくつかの理由に対して有利である。

【０１０３】もし単一レベルの暗号化が使用されたとして、送り主が受取人の公開キーを使用する場合、受取人だけが、メッセージを復号化できることになり、これは望ましい特性の１つである。しかし、受取人は、もう１つのデジタル署名無しには、送り主であると述べる者が実際に本当の送り主であることを確実にするためのすべがないであろう。

【０１０４】受取人の公開キーを使用する代わりに、送り主がその秘密キーを使用すると仮定する。すると、受取人は送り主の公開キーを使用して、メッセージを復号化することができ、メッセージを送ることができた、ということだけを知ることになり、他の望ましい特性となる。しかし、これも問題があり、送り主の公開キーの知識を持つ他人も（公開キーは公開されているから、誰にでもなりうる）メッセージを復号化できることになる。

【０１０５】本発明に従う二重暗号化の使用は、デジタルグラフィック署名の概念を外れたところに影響を及ぼすので、新規性があり無比である。デジタルグラフィック印鑑は、文書の要素であることができ、それ故に、使用方法は融通を利かせることができる。

【０１０６】例えば、私信が短ければ、通信内容は、全てデジタルグラフィック印鑑に包含することができる。文書の要約は、詳細ではなく、一般的な内容を伝達するのに使用されるであろう。文書の本文は、空白または要約のコピーであってもよい。

【０１０７】長い私信では、対称キーが、文書の本文を復号化するのに使用されるよう、デジタルグラフィック印鑑内で暗号化することができる。これは、従来の暗号方式の文献に記述されている「セッションキー」に似ていなくもない。デジタルグラフィック印鑑の融通性の他の利点は、オンラインセッションにおけるように同期的に使用できこと、あるいは電子メール文書でのように非同期的に使用できることである。

【０１０８】デジタルグラフィック印鑑は、あらゆる取引で使用できるが、その利益は、実際のオンラインセッションキーを通信するために利用される通信以外の通信において見出される。何故なら、利用可能な既に強固な技術があるからであり（例えば、ディフィーヘルマン Diffie-Hellman）、そのタイプのセキュリティは、ネットワーク通信の低いレベル（トランスポート層対アプリケーション層）にあるのが普通だからである。デジタルグラフィック印鑑は、セキュリティを増すために従来のセッションキーに加えて使用することができるであろう。一旦、受取人のサーバーに受取られても、内容の暗号化を維持し、明文になるのを防ぐことが意図されている場合に、これは特に有利である。

【０１０９】例えば、銀行の顧客が、インターネット上でＡＴＭ　ＰＩＮを変更したいとする。文書は、銀行への顧客の指図を示すだけのごく一般的な要約を含むであろう。ＡＴＭ　ＰＩＮ変更は、短いメッセージであるから、印鑑は、前述のとおり、レッドカラー値へ符号化された、必要な口座番号、古いＰＩＮ、および新しいＰＩＮを有しているだろう。所定の適切な普及暗号化技術が使われるとすると、暗号化の強さは強固であり、送り主は認証されることができ、意図された受取人（銀行）だけが、取引の詳細を見ることができるであろう。明文の要約は、取引のプライバシーまたはセキュリティを傷つけられることなく、取引を復号化して処理するのに適する安全な環境へ印鑑を送るのに充分な情報を、銀行の処理センターに与えるであろう。

【０１１０】本発明の好ましい実施形態および特徴を参照して説明してきたが、類似する他の実施形態および特徴が類似の結果を得るのに利用されてもよい。本発明の変更および修正は、当該技術に精通する者にとっては明らかであり、本発明の開示は、以下の特許請求の範囲の適用範囲内で、そのような変更および修正の全てを包含することを意図する。

【図面の簡単な説明】

【図１】図１は、本発明のデジタルグラフィック署名の実施形態を示す。

【図２】図２は、本発明のデジタルグラフィック署名システムの実施形態の概略図である。

【図３】図３は、本発明のデジタルグラフィック署名システムのデジタルグラフィック署名ダイアログ機能のフローチャートである。

【図４】図４は、本発明のデジタルグラフィック署名システムにおける、署名前の文書要約の画面サンプルである。

【図５】図５は、本発明のデジタルグラフィック署名システムにおける、文書本文の画面サンプルである。

【図６】図６は、本発明のデジタルグラフィック署名システムにおける、署名前の署名領域の画面サンプルである。

【図７】図７は、本発明のデジタルグラフィック署名システムにおける、署名後の署名領域の画面サンプルである。

【図８】図８は、本発明のデジタルグラフィック署名システムの署名者認証機能のフローチャートである。

【図９】図９は、本発明のデジタルグラフィック署名システムにおける、認証前の署名領域の画面サンプルである。

【図１０】図１０は、本発明のデジタルグラフィック署名システムにおける、認証後の署名領域の画面サンプルである。

【図１１】図１１は、本発明のデジタルグラフィック署

名システムの公開署名者認証機能のフローチャートである。

【図１２】図１２は、本発明のデジタルグラフィック印鑑を含むデジタルグラフィック署名システムの実施形態の概略図である。

【図１】

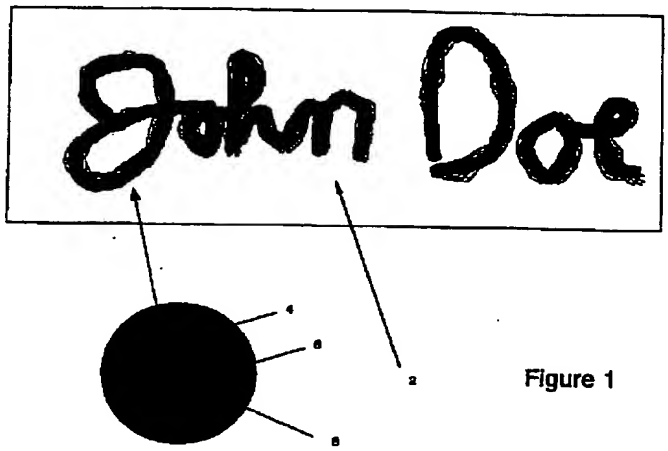
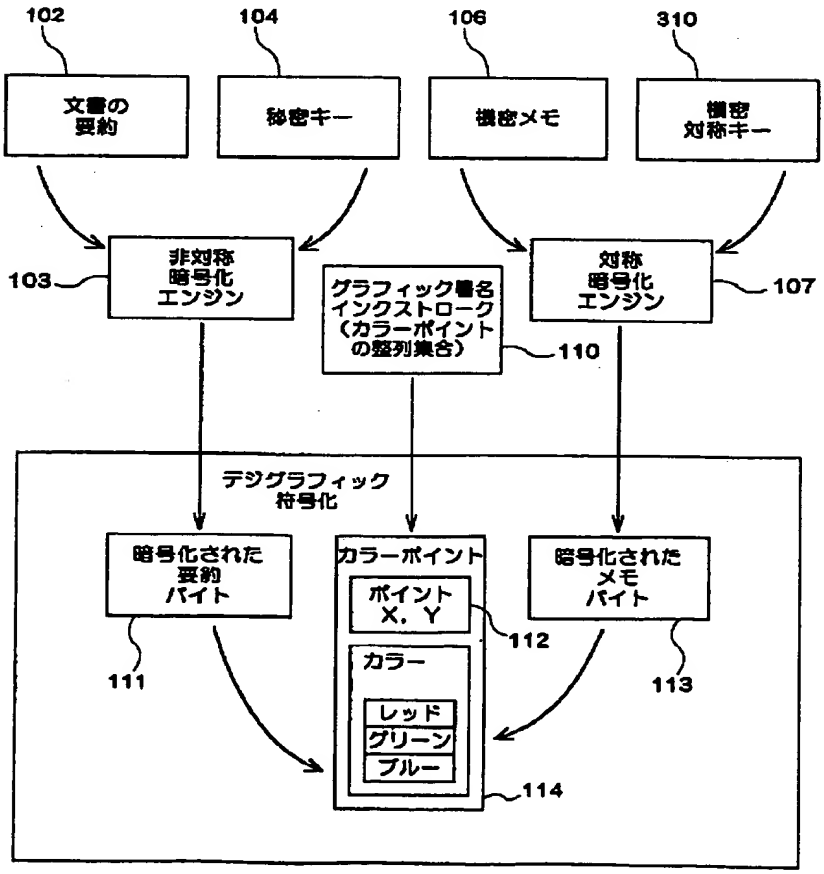
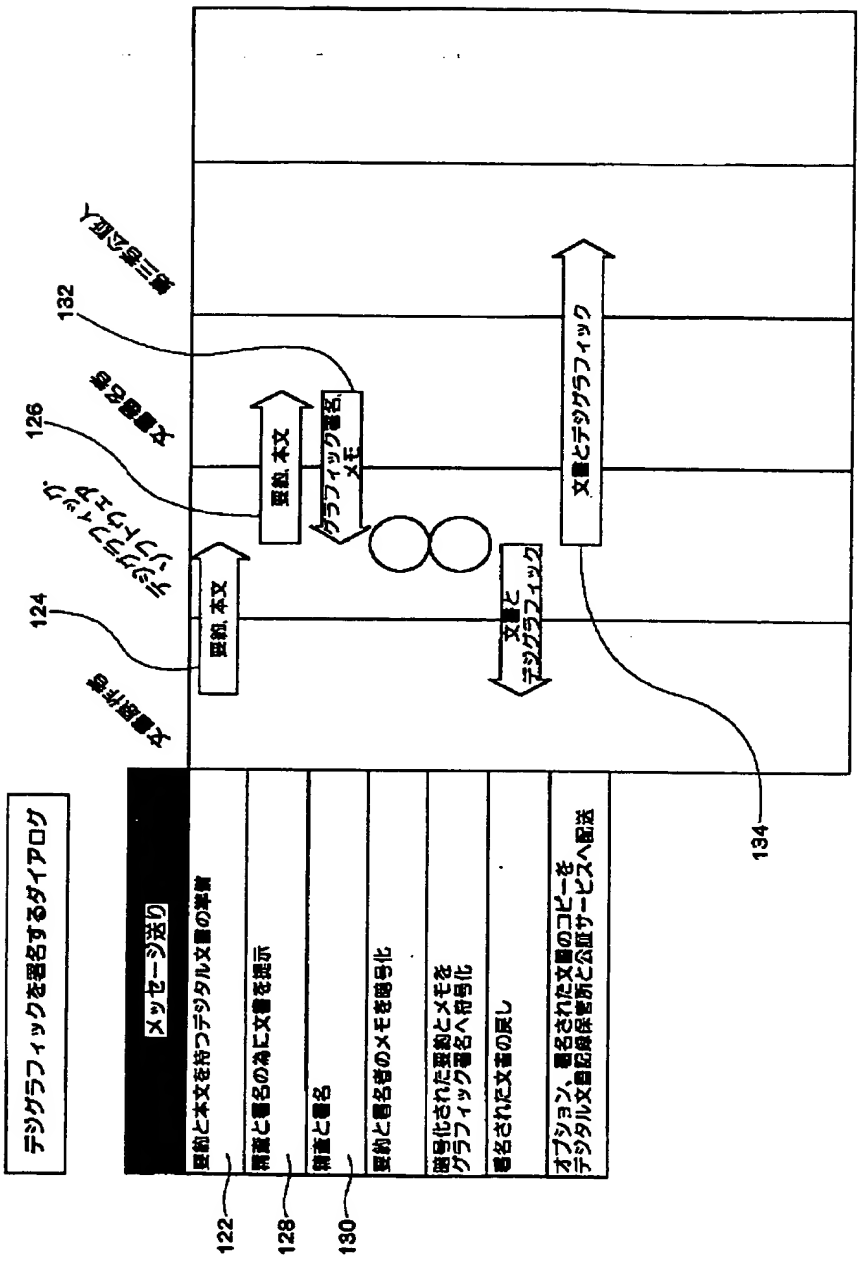


Figure 1

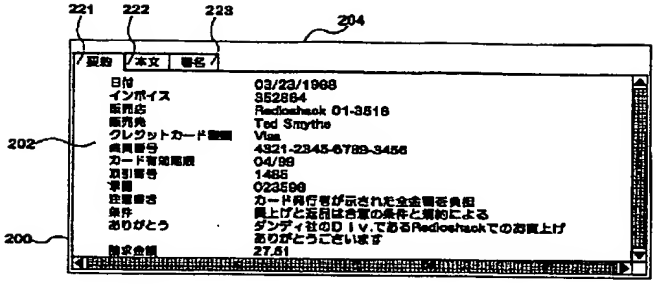
【図２】



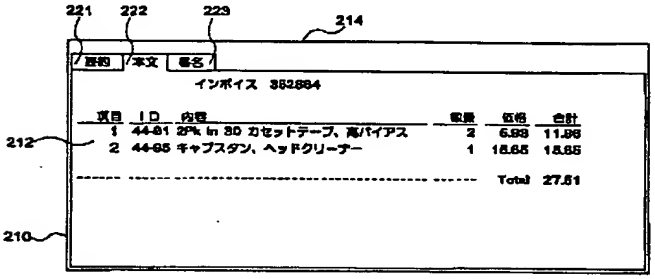
【図３】


デジグラフィックを署名するダイアログ
メッセージ送り
要約と本文を持つデジタル文書の準備
精査と署名の為に文書を提示
精査と署名
要約と署名者のメモを暗号化
暗号化された要約とメモを
グラフィック署名へ符号化
署名された文書の戻し
オプション、署名された文書のコピーを
デジタル文書記録保管所と公証サービスへ配送
122
128
130
文書処理作業
要約 本文
124
デジグラフィック署名
126
署名確認文
要約 本文
グラフィック署名 メモ
132
第三者公証人
文書とデジグラフィック
文書とデジグラフィック
134

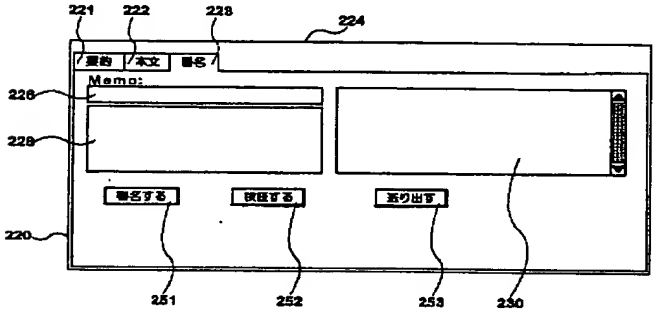
【図４】


221
222
223
204
要約
本文
署名
日付 03/23/1998
インボイス 352884
販売店 Redoshack 01-3516
販売先 Ted Smythe
クレジットカード種類 Visa
会員番号 4321-2345-6789-3456
カード有効期限 04/99
取引番号 1485
承認 023596
注意書き カード発行者が示された全金額を負担
条件 売上げと返品は当社の条件と規約による
ありがとう ダンディ社のＤｉｖ.であるRedoshackでのお買上げ ありがとうございます
202
200
請求金額 27.51

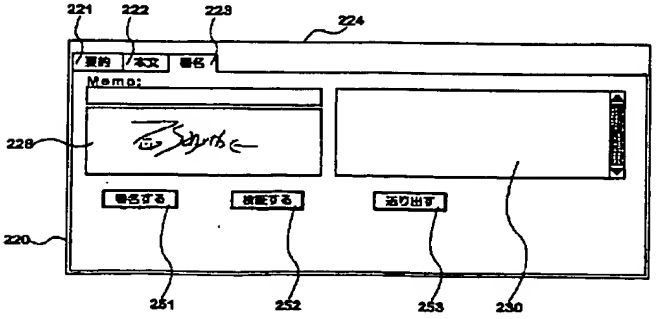
【図５】


221
222
223
214
要約
本文
署名
インボイス 352884
項目 ＩＤ 内容 数量 価格 合計
1 44-01 2Pk in 30 カセットテープ、高バイアス 2 6.93 11.86
2 44-65 キャプスタン、ヘッドクリーナー 1 18.65 18.65
Total 27.51
212
210

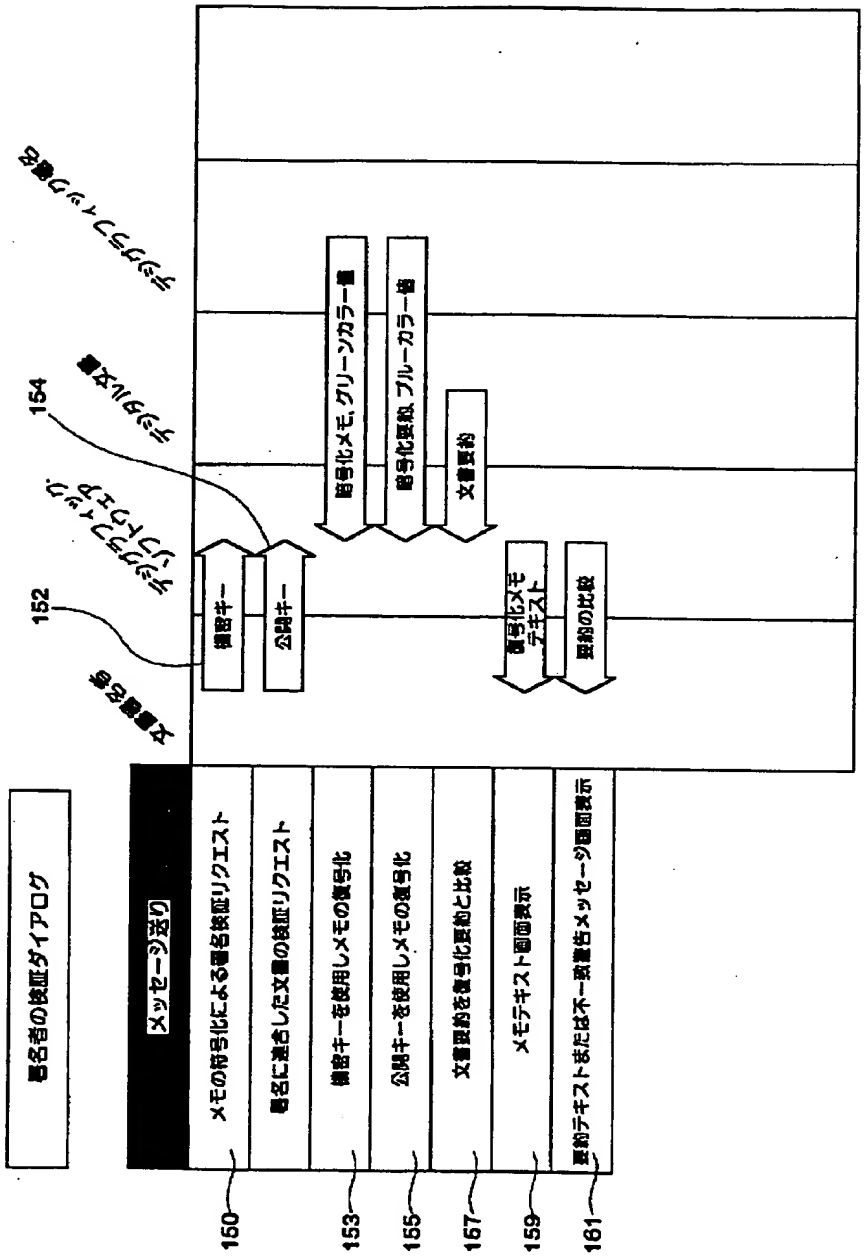
【図６】


221
222
223
224
要約
本文
署名
Memo:
226
228
署名する
検証する
送り出す
220
251
252
253
230

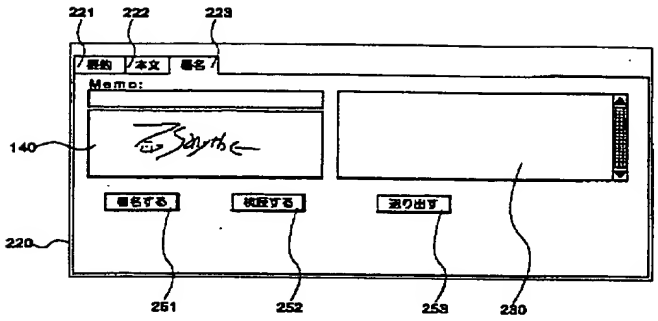
【図７】


221
222
223
224
要約
本文
署名
Memo:
228
署名する
検証する
送り出す
220
251
252
253
230

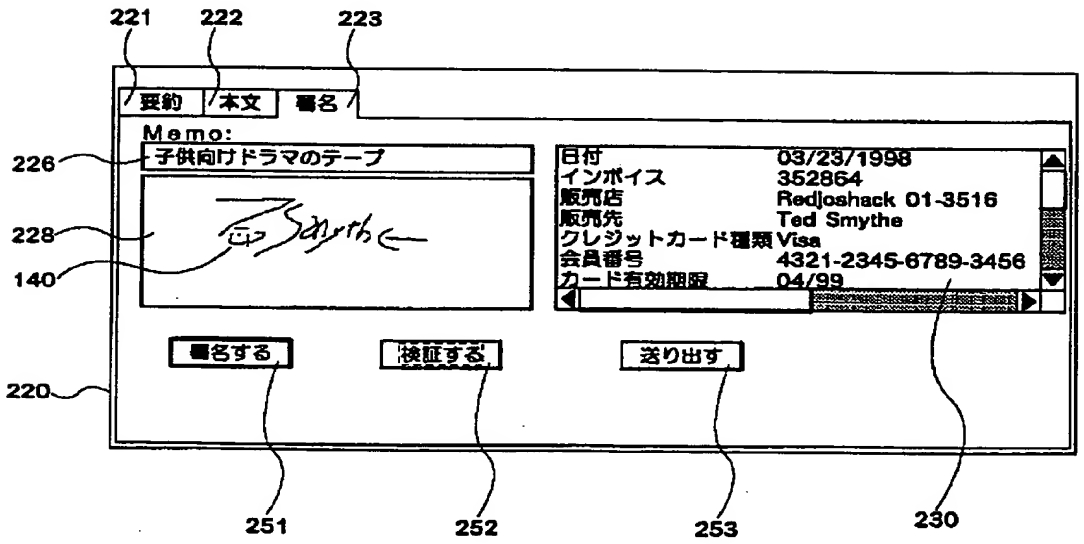
【図８】


署名者の検証ダイアログ
メッセージ送り
メモの符号化による署名検証リクエスト
署名に選ばした文書の検証リクエスト
暗号キーを使用しメモの復号化
公開キーを使用しメモの復号化
文書要約を復号化要約と比較
メモテキスト画面表示
要約テキストまたは不一致警告メッセージ画面表示
150
153
155
167
159
161
暗号化メモ、グリーンカラー値
暗号化要約、ブルーカラー値
文書要約
暗号化メモテキスト
要約の比較
暗号キー
公開キー
152
154

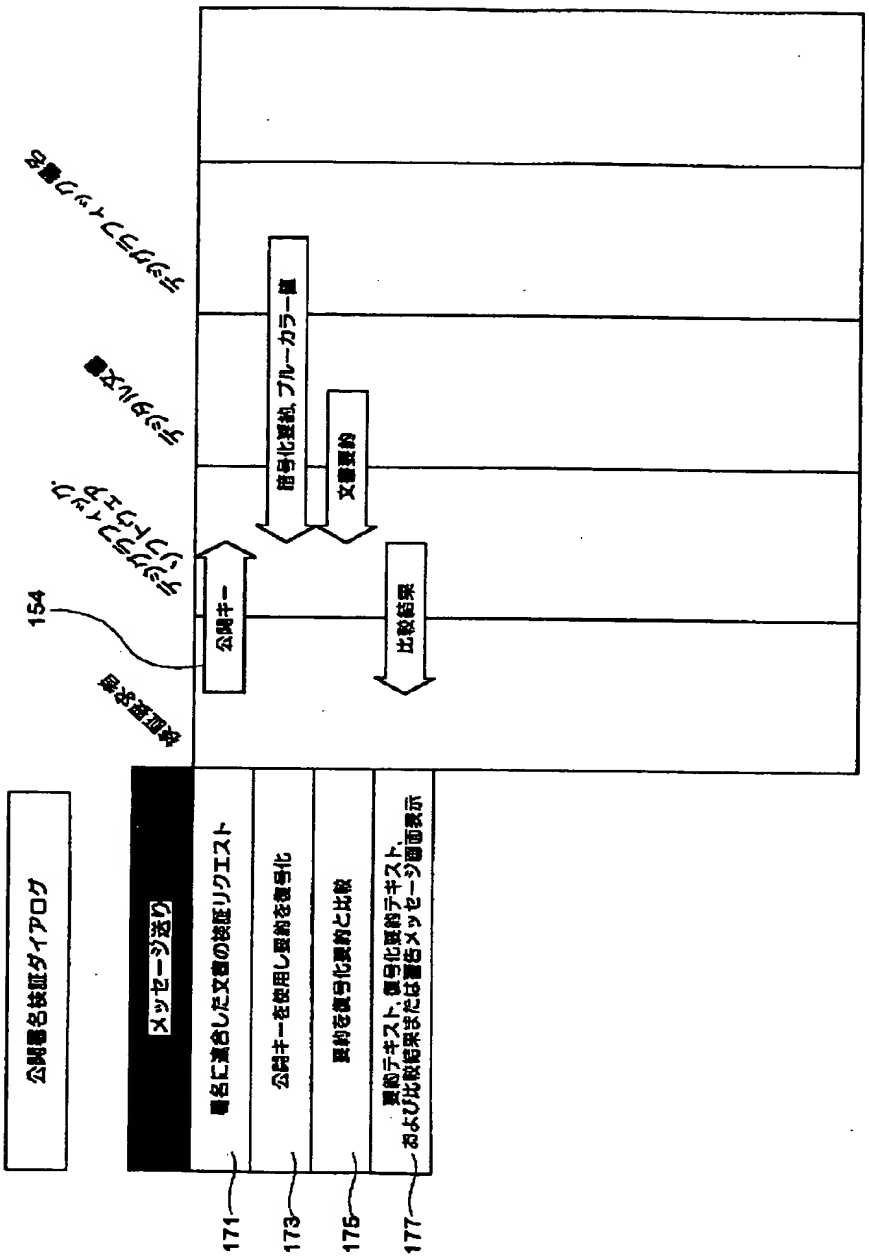
【図９】


221
222
223
要約
本文
署名
Memo:
140
署名する
検証する
送り出す
220
251
252
253
230

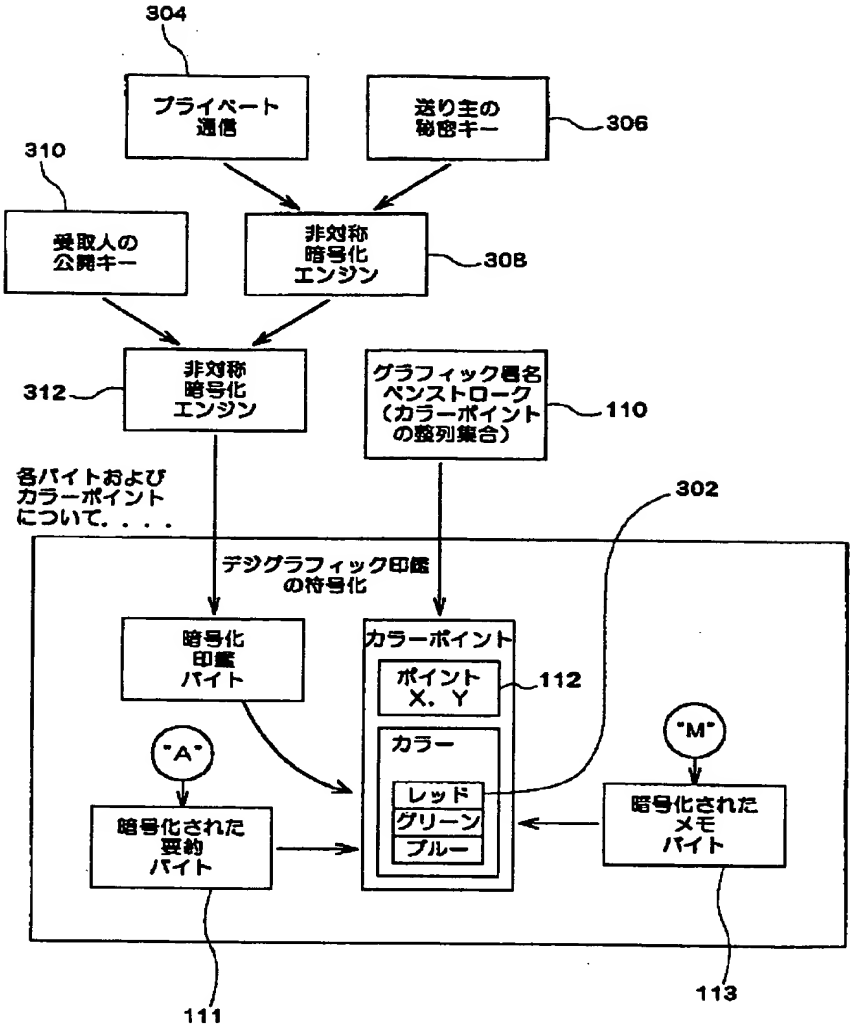
【図１０】


221
222
223
要約
本文
署名
Memo:
226
子供向けドラマのテープ
228
140
日付 03/23/1998
インボイス 352864
販売店 Redjoshack 01-3516
販売先 Ted Smythe
クレジットカード種類 Visa
会員番号 4321-2345-6789-3456
カード有効期限 04/99
署名する
検証する
送り出す
220
251
252
253
230

【図１１】


公開署名検証ダイアログ
メッセージ送り
署名に適合した文書の検証リクエスト
公開キーを使用し要約を復号化
要約を復号化要約と比較
要約テキスト、復号化要約テキスト、
および比較結果または署名メッセージ画面表示
171
173
175
177
公開キー
比較結果
署名検証要求
154
署名化要約、ブルーカラー値
文書要約

【図１２】



フロントページの続き

(31)優先権主張番号　０９／２９０４２７
(32)優先日　平成11年４月13日(1999．４．13)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　598156527
12731 W．Jefferson Boulevard，Los Angeles，California 90066，U．S．A．
(72)発明者　クリス　ティ．パルテンゲ
アメリカ合衆国　カリフォルニア州　91326，ノースリッジ，エントレイド　アヴェニュー　11718

【外国語明細書】

Digital Graphic Signature System

Cross-reference to Related Applications:

The present application claims priority under 35 USC 119(e) from US Provisional Patent Application No. 60/081,748 entitled "VIRTUAL WALLET SYSTEM" filed April 14, 1998, the disclosure of which is hereby incorporated herein by reference. The present application claims priority under 35 USC 120 from US patent application serial number 09/190,993 filed November 12, 1998, entitled "Virtual Wallet System "; and US patent application serial number 09/190,727 filed November 12 1998, entitled "Information Banking".

Field of the Invention:

The present invention relates to a digital graphic signature system for use in electronic commerce. The system comprises a document portion, including information relating to the document being executed, and a signature portion. The document portion and the signature portion may be encrypted and merged into a single object readily identifiable to an individual. The terminology "digital graphic signature" or "digigraphic signature" is utilized herein to describe the merged object.

The digital graphic signature system of the present invention may be advantageously utilized in electronic transactions, including transactions over the internet and network systems. The digital graphic signature system of the present invention may also be advantageously utilized in conjunction with information banking and virtual wallets.

The present invention also relates to a digital graphic signet that may be utilized to transmit a private communication.

Background:

In the physical world, signatures are easily recognized, particularly by their owners. The authenticity of such physical signatures, however, may be difficult to verify.

In contrast, in the digital world, digital signatures are sufficiently verifiable to support non-repudiation, using modern public key crytpgraphic techniques. Such digital signatures however may not be in a form recognizable to humans. Thus a need exists for a digital signature system that permits an individual to visually recognize their own signature. In addition to this problem, there are several other problems that need addressing in the electronic commerce and electronic financial transaction worlds.

A first problem relates to provide information to a consumer regarding the substance of a digital document to be executed. This problem may be phrased as "How does a consumer know what he or she is signing when the "document" being presented is digital?".

An additional problem relates to a consumer associating their digital signature with a digital document. This problem may be phrased as "How does a consumer recognize his or her own digital signature that has been associated with a digital document?".

For financial institutions, merchants, vendors and/or others engaged in electronic and non-electronic commerce, problems arise when a consumer fails to remember they have executed a transaction. This situation may arise in part due to the length of time between the transaction and the consumer receiving a billing statement

that includes the transaction. Many customer service calls are received from consumers requesting additional documentation regarding specific transactions on their billing statements. Often the consumers have good intentions and literally do not remember the transaction. Upon receipt of a document showing the nature of the transaction, and their signature, a consumer will generally be able to remember the transaction, or recognize the transaction as fraudulent. This process, however, is costly for institutions as it involves maintaining a customer service infrastructures, including personnel, document processing and mailing capabilities.

Problems and costs that exist today in the physical world are likely to become worse in the electronic transaction arena. A particular problem with many current technologies is that consumers are not provided with visual feedback of their signature executing a document or agreement. Also the data provided in billing for electronic transactions may not provide sufficient data for a consumer to recall a transaction.

The foregoing problems, and others, are addressed by the systems of the present invention.

Summary of the Invention:

The present invention provides a system that allows individuals to recognize their signatures on electronic documents, and provides information relating to the document, that may enable the individual to understand the document being signed and recall their execution of the document at a later date.

According to the present invention, a digital graphic (digigraphic) signature system comprises a graphic formed by combining details relating to the document being executed, and an individual's signature. The document details and the

individual's signature may be encrypted utilizing conventional techniques to provide enhanced security. The digital graphic signature may be displayed through a user interface for inspection.

Document details that may be incorporated into the digigraphic signature include:

an abstract of the document being executed;

the body of the document being executed;

excerpts from the body of the document being executed; or

an individual's notes relating to the document being executed.

In general, it is believed advantageous for many purposes to include at least an abstract comprising a digest of what an individual is actually agreeing to by executing the document. The abstract may also include reference information, including but not limited to, the date, the parties involved, transaction reference numbers and the like. Preferably, the abstract is written in plain (non-legal) terms that are readily understandable to even relatively unsophisticated consumers. Generally, the abstract will be reduced to text for purposes of forming the digigraphic signature. However, for certain applications it may be advantageous for the abstract to include graphic or pictorial information.

For certain transactions, it may be advantageous to include the body of the document being executed, or excerpts from the body of the document being executed, in the digigraphic signature in addition to, or in place of an abstract. The document body, and/or excerpts will generally be reduced to text for purposes of forming the digigraphic signature. However, for certain applications it may be advantageous to include graphic or pictorial information.

As set forth above, document details may further comprise an personal memo area that allows an individual to record information of their own choosing about the document being executed. Preferably, the individual will enter information that will help them remember the transaction in the future. Such information could include, the purpose of the transaction, the nature of the transaction, as well as other details having significance to the individual.

A representation of an individual's signature may comprise graphical data generated from a graphic of the individual signature. An individual's signature graphic may be obtained by capturing the pen strokes utilized by an individual to sign their name, for example through the use of a graphics tablet. An individual's signature graphic may also be obtained by scanning a signature from a physical document. In general, prior to the translation and merging steps described below, an individual's signature graphic will be similar to the individual's signature on a physical document.

To produce a digital graphic signature, the document details data and the individual's signature data are merged. The merging process may include encrypting both sets of data utilizing conventional electronic encryption techniques. Different portions of the document details may be encrypted with public or private keys.

For example, it may be advantageous to encrypt document abstract data with a private key of the individual who is executing the document utilizing convention public key cryptographic techniques. The abstract could then be made accessible to the individual and the other party to the transaction.

The memo text data entered by an individual could be encrypted with a symmetric key known only to the individual. As explained below, this could provide

an addition insurance to the individual that the document is not forged and assist them in remembering the transaction.

The document detail data and the individual's signature data may then be merged, for example utilizing color encoding. In this technique, each data stream is utilized as color values, for example in standard RGB (red, green, blue) color encoding. For example, each byte of an abstract stream may be used to generate blue values, each byte of a memo stream may be utilized to generate green values. A non-changing red value may be used to complete the description. Other color values may also be utilized. For example, CMYK (cyan, magenta, yellow, black) color encoding may be utilized to produce the digital graphic signature with the cyan, magenta, yellow and black color values corresponding to data streams .

The digital graphic signature may be defined as a series of ink strokes using "color-points", a point defined by relative coordinates with respect to a defined signature area, and a color value. The relative coordinates may comprise x,y coordinates; r,θ coordinates or the like in a two dimensional signature area; or x,y,z coordinates or the like in a three dimensional signature area etc.

Initially, the individual's signature data may comprise captured strokes of a single color. During the merging process the initial color values are replaced with the encoded cryptotext values. The point positions may be retained to preserve the graphical appearance of the signature.

Differences in the length (byte count) of the signature data and the abstract and/or memo stream data may be handled by a bidirectional padding technique, or similar techniques understood to those of ordinary skill in the art.

If the signature data is longer than either of the abstract or memo data, zero values may be used for the blue and green portions and only the non zero, non changing red value used for the remainder of the signature data. In this way the graphical appearance of the signature is preserved, even when the abstract and/or memo data ends.

If the abstract data and/or the memo data is longer than the signature data, zero point values may be assigned to color-points, while the colors are used to encode the remainder of the messages. The remainder of the message need not assume the graphical representation of the signature data, but may appear as part of the digital graphic signature.

The resulting digital graphic signature may advantageously retain a visual appearance similar to an individual's physical signature, however will comprise points of red, green and blue color. The relative amounts of red, green and blue points will associate the digital graphic signature with a particular document, as the green and blue points will be generated in response to data specific to a particular document.

As will be understood by those of ordinary skill in the art, different colors, or a different color encoding scheme, may be utilized in a similar fashion to produce a digital graphic signature according to the present invention.

The digigraphic signature may be saved as a data file, for example a *.gif file; *.tiff file; *.pict file; *.jpg file; or the like, and associated and/or stored with data files for the transaction. Preferably, the digigraphic signature is saved in a file type capable of being displayed on a video monitor by popular computer software programs, such as internet browser software, financial transaction software, and/or word processing software.

Thus, in one aspect, a digital graphic signature of the present invention comprises a graphical representation of an individual signature produced from a plurality of points, wherein the plurality of points comprise at least a first set of points corresponding to information particular to a document being executed, and a second set of points corresponding to the individual's signature.

In another aspect, a digital graphic signature of the present invention comprises a visually recognizable multi-color graphical representation of an individual's signature capable of being displayed on a video monitor the graphical representation having a unique color scheme corresponding to the document being executed. As used herein the terminology video monitor includes computer video monitors, televisions and the like.

According to the present invention, a digital graphic signature system comprises a digital graphic signature of the present invention and computer software and hardware capable of generating and displaying the digital graphic signature system. The computer hardware may comprise a central processing unit, video monitor display; memory; modem; keyboard; mouse; trackpad; graphics tablet; scanner; printer and/or other generally available computer hardware components. It is generally preferred that the computer hardware include a graphics tablet; electronic pen; touch sensitive screen; mouse; trackball; joy stick; electronic pen; point-of-sale electronic pen apparatus or similar input device for capturing an individual's signature as "pen strokes". The same input device, or another input device such as a keyboard, is useful for allowing an individual to create a memo data file corresponding to the memo relating to the document being executed.

Computer software useful in systems of the present invention includes encryption software for encrypting data streams and color encoding data streams. Additional software, such as word processing programs, graphics programs, and the like may also be useful, for example, to allow an individual to enter a memo relating to the transaction, and for viewing the digital graphic signature.

The present invention also provides a method for producing a digital graphic signature corresponding to a document executed by an individual, the method comprising:

forming an abstract of the document;

obtaining the individual's signature;

producing a document abstract data stream from the abstract;

producing a signature data stream from the signature; and

merging the document abstract data stream and the signature data stream into a digital graphic signature.

The method may further comprise:

obtaining memo data from the individual;

producing a document memo data stream; and

merging the document abstract data stream, the document memo data stream and the signature data stream into a digital graphic signature.

In an alternative embodiment, the present invention provides a method for producing a digital graphic signature corresponding to a document executed by an individual, the document method comprising:

selecting details relating to the document;

forming an abstract of the document;

obtaining the individual's signature;

producing a document details data stream from the details;

producing a document abstract data stream from the abstract;

producing a signature data stream from the signature; and

merging the document details data stream; the document abstract data stream and the signature data stream into a digital graphic signature.

This method may further comprise:

obtaining memo data from the individual;

producing a document memo data stream; and

merging the document details data stream; the document abstract data stream, the document memo data stream and the signature data stream into a digital graphic signature.

The data streams may be obtained and merged utilizing the techniques described above and in greater detail below. In addition, the data streams may be encrypted.

In a further aspect, the present invention provides a method and means for providing a private communication between two parties, for example two parties to a transaction. The present invention provides a functionality referred to herein as a "digital graphic signet" or a "digigraphic signet". The digital graphic signet may provide additional functionality to the digital graphic signatures of the present invention discussed herein. As will be understood by those of ordinary skill in the art, the digital graphic signet may also be utilized independently.

As discussed herein, the digital graphic signature, systems and methods of the present invention provide increased functionality in comparison with digital

signatures and digital certificates alone. They address the consumer perceptual need to feel comfortable with signing a digital document, and to be able to recognize a digital document they have signed, while having assurances that their signature was not forged, and it was not copied from another document.

The signatures, systems and methods of the present invention add a human factor to conventional cytography that makes it recognizable and useful, for example by allowing a memo that assists the signatory in remembering the transaction. Additional benefits are that digital graphic signatures according to the present invention are generally smaller than conventional digital certificates, and therefore may be more desirable for storage purposes and to reduce network traffic loads. They are unique in the digital signature world in that their content may include representing a recognizable graphic of a handwritten signature while also containing digital signature information, using the most appropriate prevailing cryptographic techniques.

As discussed herein, a digital graphic signature of the present invention may utilize a technique similar to steganography to encode a signatory's memo in the green color bytes, and the document's abstract in the blue color bytes, into a graphic representation of their hand written signature.

The technique is not necessarily technically steganography as it is not strictly necessary to hide the fact that there are messages present and encoded into the graphic. Therefore, DigiGraphic signatures do not attempt to hide the content of a communication between two or more parties. The memo is intended only for the signatory's use, and uses a secret key known only to the signatory. Any third party with the signatory's public key can verify the signature. Its purpose is for the authentication of the signatory, and to ensure non-repudiable transactions, not for

encryption of private communications. It should be understood, however, that it is possible to encrypt a digital graphic signature of the present invention and such embodiments fall within the scope of the present invention. An advantage of embodiments of the present invention is that further encryption may not be necessary.

The terminology digital graphic "signet" is borrowed from the ancient notion of a signet ring, which was used to seal a private communication between two parties. The analogy breaks down quickly, however, for in the ancient world, a broken seal indicated that the privacy had been compromised. It could not prevent the privacy from being compromised. According to the present invention a digital graphic signet is an embodiment of a digital graphic signature of the present invention that further includes a confidential communication between two parties. The digital graphic signet utilizes a color value, for example the red color value in a RGB color scheme for the encoding and transmitting of a confidential communication. Further details are set forth below.

A digital graphic signet of the present invention may also be utilized in a method of the present invention by encoding a confidential communication in a data stream.

The digital graphic signature, digital graphic signet, systems and methods of the present invention may be advantageously utilized in electronic transactions, including transactions over the internet and network systems. The digital graphic signature system of the present invention may also be advantageously utilized in conjunction with information banking and virtual wallets such as those described in US patent application serial number 09/190,993 filed November 12, 1998, entitled "Virtual Wallet System "; and US patent application serial number 09/190,727 filed

November 12 1998, entitled "Information Banking" and related technologies described in US patent application serial number 09/###,###, filed April ##, 1999, entitled "System and Method for Securely Storing Electronic Data"; and US patent application serial number 09/###,###, filed April ##, 1999, entitled "System and Method for Controlling Transmission of Stored Information to Internet Websites". The disclosure of each of these applications is hereby incorporated herein by reference.

The advantages of the digital graphic signature system and method of the present invention include the following.

An individual may visually recognize their own signature.

In previous alternatives, a graphic could be included with the document of the individual's signature. However, traditional graphics are easily copied and therefore relatively simple to forge. Additionally, there is nothing inherent about a traditional graphic that securely associates the graphic with a document being executed. In contrast, the digital graphic signature created utilizing the present invention is relatively difficult to forge and associated with the document being executed.

An additional advantage is that the digital graphic signature of the present invention may be verified. To verify that the individual was indeed the person who executed the document, the known, public key could be utilized to decrypt the abstract portion of the signature. According to the present invention, this abstract is encoded into the graphic signature. The abstract should match exactly the document abstract that is not encrypted in the document. This demonstrates that the document was signed by the consumer (because they were the only person in possession of the

private key that produced the signature) and that the disnature is associated to a specific document due to the abstracts matching.

In addition, the individual may use their secret key to read the memo encoded into the graphic signature. Insofar as the memo is not in the document, and cannot be decrypted by anyone else, unlike the abstract, the memo provides the individual with an additional assurance that the document was not forged. The memo may also assist the individual in remembering the document.

An advantage of a digital graphic signet embodiment of the present invention is that a digital graphic signature may include a confidential communication between two parties.

Further details and advantages of the present invention will become apparent from the following description and the appended figures.

Brief Description of the Drawings:

Figure 1 depicts an embodiment of a digital graphic signature of the present invention.

Figure 2 is a schematic representation of an embodiment of a digital graphic signature system of the present invention.

Figure 3 is a flowchart of a digital graphic signing dialog function of a digital graphic signature system of the present invention.

Figure 4 is a sample screenshot of a document abstract before signing in a digital graphic signature system of the present invention.

Figure 5 is a sample screenshot of a document body in a digital graphic signature system of the present invention.

Figure 6 is a sample screenshot of a signature area before signing in a digital graphic signature system of the present invention.

Figure 7 is a sample screenshot of a signature area post signing in a digital graphic signature system of the present invention.

Figure 8 is a flowchart of a signatory verification function of a digital graphic signature system of the present invention.

Figure 9 is a sample screenshot of a signature area pre-verification in a digital graphic signature system of the present invention.

Figure 10 is a sample screenshot of a signature area post verification in a digital graphic signature system of the present invention.

Figure 11 is a flowchart of a public signatory verification function of a digital graphic signature system of the present invention.

Figure 12 is a schematic representation of an embodiment of a digital graphic signature system including a digital graphic signet of the present invention.

Detailed Description of the Invention:

The features and advantages of the digital graphic signature systems and method of the present invention are explained in the following paragraphs with reference to the Figures.

Figure 1 depicts a possible embodiment of an individual's, "John Doe", digital graphic signature according to the present invention. As shown in Figure 1, a digital graphic signature of the present invention has a visual appearance, 2, similar to an individual's written signature. As shown in the cut-away view, the visual representation is formed by individual points in a plurality of different colors. For

example, the visual representation may be formed by green points 4, blue points 8, and red points 6. The relative number and position of the points of each color will be unique for each transaction and based on the relative amounts and kind of document data and signature data that is color coded to produce the digital graphic signature. In general, however, the overall visual representation will be similar to an individual's written signature to simplify identification.

A simple embodiment of a DigiGraphic signature includes a graphical user interface (GUI or simply UI) that allows a user to see:

1) an abstract of the document to be signed;

2) the body or detail of the document to be signed;

3) a signature pad area to graphically sign their name

4) a personal memo area.

The abstract may comprise a digest of what a consumer is actually agreeing to by signing the document. The abstract is preferably in plain (non-legal) terms, and reduced to a text representation (devoid or graphics etc.). In effect, the abstract is actually what is being signed. The abstract may additionally include other relevant items including for example the date and the names of the parties to the agreement.

Once a consumer has read the document and has made a decision to sign, they move to the signature area and graphically sign their name. Additionally, the consumer may be encouraged to enter a memo in the personal memo area to remember the transaction they are executing.

The pen strokes utilized to sign the document, and the memo, are captured via a computer system, hardware and software. In addition, the computer system will

encode the text of the abstract and the memo into the graphic signature. A preferred technique is similar to steganography.

First the two message streams are encrypted using modern cryptography. The abstract may be encrypted with the consumer's private key using modern public key cryptographic techniques. The memo text may be encrypted using a symmetric key known only to the consumer.

The two encrypted streams are than used as color values in standard red, green, blue (RGB) color encoding. For example, each byte of the abstract stream would be used for the blue values, which the memo stream byte values are sued for the green values. A non changing red value would be used to complete the color description.

The graphical signature is defined as a series of ink strokes using "Color-Points". a point (relative x and y coordinates with respect to a defined signature area), and a color value. The capture ink strokes are initially captured in a single color. During the encoding process, the color values are replaced with the encoded cryptotext values. The point positions are retained, of course, to preserve the graphical appearance of the signature.

Differences in the length (byte count) of the graphical signature strokes and the abstract and memo streams are handled by bidirectional padding. If the graphical signature is longer than either of the two messages, zero values are used for the blue and green portions and only the non zero, non changing red value is used. In this way the graphic appearance of the signature is preserved, even when the messages end. If one of the messages is longer than the graphical signature, zero point values are assigned to Color-points, while the colors are still used to encode the rest of the message(s). The interface is designed not to attempt to draw strokes that have no

positional value, but the non-drawn portion of the signature still preserves the messages.

The graphical representation of the users signatures has been merged with a digital signature into a single object. This merged object has several advantages, including the following.

Consumers can visually recognize their own signatures. In previous alternatives, a graphic might be included with the document of the consumer's signature. However, normal graphics are easily copied, and therefore forged. Additionally, there is little inherent about a conventional graphic that securely associates it with a document.

To verify that the consumer was indeed the person who signed the document, the a public key of the consumer can be utilized to decrypt the abstract portion of the signature. The digitally signed abstract is encoded into the graphic signature. Additionally the abstract should match exactly the document abstract that is "in the clear" or not encrypted in the document. This matching demonstrates that the signature 1) was signed by the consumer (because they were the only person in possession of the private key that made the signature) and 2) that the signature is associated with a particular document due to the abstracts matching.

In addition, a consumer may use their secret key to read the memo encoded into the graphic signature. Since the memo is not in the document and cannot be decrypted by others, unlike the abstract, the memo is an additional assurance to the consumer that the document was not forged and also helps them remember the transaction.

Figure 2 provides a schematic representation of a process for producing digital graphic (DigiGraphic) signatures. As shown in Figure 2, an embodiment of a DigiGraphic signature process according to the present invention includes a document abstract, 102 which is encrypted using a private key 104, in an asymmetric encryption engine 103. The process may further include a secret memo 106 which is encrypted using a secret symmetric key 108 in a symmetric encryption engine 107. The encrypted abstract and/or encrypted memo may then be encoded with graphic signature ink strokes (an ordered collection of Color-Points), 110 produced by a person's signature on a signature pad.

The two encrypted streams are used as color values in a standard RGB color encoding as described above. In Figure 2 the encrypted abstract bytes 111 correspond to blue and the encrypted memo bytes 113 correspond to green. The graphic signature is defined as a series of ink strokes using color points 112, in the manner described above. The resulting object comprises a merger of the person's signature with a digital signature into a single object 114.

Figure 3 depicts a schematic flowchart of the DigiGraphic signing dialog. The message sends illustrated in the flowchart would be implemented in software and respond to input from a person using the DigiGraphic signing feature. As shown in Figure 3, an initial step, or message send, is to prepare a digital document with abstract and body 122. In this step the document originating software forwards, or inputs, 124, the body of a document, and an abstract, to the DigiGraphic software. The document is then read by the DigiGraphic software which generates a document abstract and a document body, 126. A sample document abstract is depicted in Figure 4 for Ted Smythe, and a sample document body is depicted in Figure 5.

As shown in Figure 4, a document abstract 200, may include details 202 relating to the document being executed in a Windows® display 204 which includes tabs 221 ("Abstract"), 222 ("Body") and 223 ("Signature"). Under the "Abstract" tab, a document abstract 200 may include factual details relating to the transaction, including, but not limited to the details shown in Figure 4:

Date	03/23/1998
Invoice	352864
Merchant	Radioshack 01-3516
Sold To	Ted Smythe
Credit Card Type	Visa
Account	4321-2345-6789-3456
expires	04/99
Transaction #	1485
Authorization	023598
Note	The card issuer may apply the total amount shown
Terms	Sales & returns are subject to terms & conditions agreed to.
Thank You	Thank you for shopping at Radio Shack ...
Amount Due	27.51

Figure 5 depicts a sample document body 210 for the sample transaction, the abstract of which is shown in Figure 4. As shown in Figure 5, a document body may include text details 212 of the document body of the document being executed in a Windows® display 214 which includes tabs 221 ("Abstract"), 222 ("Body") and 223 ("Signature"). The document body 212 may be displayed under the "Body" tab.

Referring back to Figure 3, the person signing the document would review, 128, the document abstract and body and then prompted to enter a memo which will help them remember the document, followed by their signature 130. Figure 6 depicts a possible embodiment of the user interface which prompts for a memo and signature.

As shown in Figure 6, a signature user interface 220 may be executed in a Windows® display 224 which includes tabs 221 ("Abstract"), 222 ("Body") and 223 ("Signature"). Under the "Signature" tab, a signature user interface 220 may include a Memo area, 226, a graphic signature area 228 and an memo entry area, 230 where an individual may enter a personal memo relating to the document being executed. The memo entry area 230 may initially include a text prompt, prompting a user to enter a personal memo. The interface 220 may further include "buttons" 251 ("Sign"), 252 ("Verify") and 253 ("Submit") which are linked to implementing routines to enable a user to sign, verify and submit their signature.

Post signing, the private memo entered by the user, and the document abstract are returned to the digigraphic signature 132 encoded into the user's signature. Figure 7 depicts a possible embodiment of an encoded graphic signature, 140 for user "Ted Smythe". The user is then prompted, for example by a text prompt in window 230, to submit the encoded graphic signature to the document originator to "sign" the document and complete the transaction between the user and the document originator. As shown in Figure 3, 134, the signed document and digital graphic signature may optionally be delivered to a digital document archive or a notary service for verifying the digital signature. The notary service would utilize the signer's public key to verify that the signature has not been forged.

A digital graphic signature system of the present invention may be advantageously utilized in a virtual wallet system, such as the system described in U.S. patent application serial number 09/190,993 filed November 12, 1998, the disclosure of which is hereby incorporated herein by reference.

In a virtual wallet the wallet owner's signature may be advantageously attached to the invoice or receipt in a format that can be recognized by the owner. The format of the final signed document of the present invention goes beyond a typical digital signature by enabling the digital signature to be humanly recognizable. The format of the final signed document enables the owner to visibly distinguish a signature as their own, associate the signature with a particular document, and verify that the signature and document are not forged or copied. The signature comprises a DigiGraphic signature of the present invention and comprises digital signatures and graphics that the wallet owner recognizes as their own. The feature of providing a recognizable and distinguishable digital signature in an electronic document is unique, and akin to the wallet owner recognizing their own hand-written signature in a paper document. This feature helps the wallet owner remember particular transactions and verify their own signature. Further details relating to digital graphic signatures are set forth above.

Notwithstanding the format, it is recommended for a document that needs to be signed that the document comprises at least an abstract and a body. The abstract, also known as the abstract in the clear, comprises a digest of what the consumer is agreeing to when they sign the document, presented in plain, non-graphical text. The abstract may be information concerning the payment, the delivery or the terms and conditions of the transaction, or other similar information. For example, payment

information in the abstract may include the date, the parties involved, the general nature of the transaction, and the payment amount. The body comprises the full amount of formatted information that is normally referred to as the document. The body, therefore, comprises all of the details associated with the transaction. Once the document is signed, it has at least three components: the abstract, the body and the signature. There may, however, be other components, such as a general terms and conditions section, shipping information, etc. So, by sending this formatted information to an appropriately enabled browser, for example, an invoice can be rendered for the wallet owner.

In operation, referring to Figure 3, the signature requester, such as a restaurant, wants the wallet owner to sign a document, such as a receipt. The requester initiates the dialogue and sends a document and an abstract. A feature of the present invention specially formats the document and the abstract and designates it as a signature document for recognition by the software. The wallet server sends the signature document to the wallet interface when it comes on line, thereby supporting both synchronous and asynchronous dialogs. The wallet interface displays the signature document and abstract to the wallet owner for signing. The owner then picks one of their signature key nicknames, or in other words the persona that they are signing with, and they graphically sign the document. The chip device encrypts the abstract with a private key and the memo with a secret key. This allows anyone with public key matching the private key to access the document, while the memo is kept confidential to the owner and anyone else who is given access to the secret key, which may or may not be the public key. The signed document now comprises the body, abstract and the DigiGraphic Signature (DS). The DS includes the digital signature by

virtue of the abstract being encrypted with the private key.

Further, the chip device passes the signed document and the associated index back to the wallet server. The chip device is tasked with remembering the index so that the wallet owner does not have to worry about it. The wallet owner can even be off-line. The wallet server archives the signed document and forwards the index, the document identification, and the signature guarantor URL to the signature requester, who stores this information. Finally, the requester acknowledges the receipt of the information. Thus, this feature of the present invention advantageously manages multiple signature keys and their associated indexes.

When the preferred DigiGraphic signature is used to sign a document, as described herein, the DigiGraphic signature object knows how to render a graphic of the signature when requested to do so. The DigiGraphic signature also contains the digital signature. The DigiGraphic signature encapsulates the behavior for third parties to perform signature verifications and for the document signer to verify their own signature and the validity of its association to the document. Further, as one skilled in the art will recognize from the description below, the preferred DigiGraphic signature advantageously serves to authenticate and authorize a document, eliminating the need for bulky digital certificates.

Figure 8 is a flowchart illustrating a possible verification document for use when the person who signed a document (the signatory) is not sure that they actually signed the document, or does not remember the transaction and desires to view the encrypted memo. Upon retrieval of a document, the signatory may view the signature, 140 on the document. A possible embodiment is shown in Figure 9 in interface 220. The user may be prompted, for example in window 230 in Figure 9, to

request signature verification 150 (Figure 8). Upon requesting verification the potential signatory's (verifier's) secret key 152 is utilized to decode the memo accompanying the signature 153. In order to use the secret key the user's would be prompted to enter a password. The potential signatory's public key, 154 is utilized to decode the signature and the document abstract 155. The decoded memo and the document abstract are then compared to the actual memo and document abstract 157 and if they match are displayed to the signatory, for example in windows 228 and 230 in Figure 9 to allow the signatory to verify that they have signed the document, 159. A possible embodiment is shown in Figure 10.

As shown in Figure 10, a signature 140 ("Ted Smythe") may be displayed in window 228, a personal memo displayed in window 226 and a document abstract in window 230. In Figure 10, the document abstract corresponds to the abstract depicted in Figure 4.

If the memo, abstract and/or signature are not decodable, or do not match the document's, a warning message may be displayed to the user and the signatory may notify the document originator of a potential forgery 161.

Another feature of the present invention, referring to Figure 8, advantageously further addresses the consumer feeling for the need to recognize their own digital signature. When a wallet owner wants to verify the authenticity of their signature on a signed document, then the local signature verification feature is utilized. Alternatively or additionally, the system may automatically verify the signature every time a document is opened, and only alert the wallet owner whenever there is a mismatch. For example, the warning may say something like "The signature does not match the abstract."

In the present case, the wallet owner retrieves a document and abstract from the document archive, which may reside on the owner's personal computer, in the wallet server, or in other similar devices. As discussed above, preferably the document is signed utilizing the DigiGraphic Signature. The wallet owner wants to make sure the signature is not forged, for example, and requests verification. The wallet interface sends a public key request to the secure chip device, which returns the key that was previously stored in association with the document. The interface then uses the key to decrypt the digital portion of the signature, comprising the abstract. The interface compares the decrypted abstract information to that of the abstract in the clear, or the abstract that is not encrypted in the document. That comparison demonstrates that the signature was signed by the owner because they were the only person in possession of the private key that made the signature, and that the signature is associated to that specific document due to the matching abstracts. Further, the graphic portion of the signature is recognizable to the owner, and the fact that the decrypted abstract, which was merged with graphical signature, matches the abstract in the clear assures the owner of it's authenticity. Thus, the wallet interface then returns a message to be viewed by the owner reporting the results of the verification check.

The combination of the digital and graphical comparison advantageously allows the signature to be verified for that particular document. This feature is unique and allows for high confidence as compared to merely checking the digital signature, which comprises bits that may be undetectably copied. Thus, this feature verifies that the DigiGraphic signature is the original signature, and not just something that looks like the original.

Additionally, this feature advantageously allows only the wallet owner to decode the memo, which is not stored anywhere else in the document, and which may contain a reminder to the wallet owner of the transaction.

Figure 11 is a flowchart of a possible public signature verification dialog for use with the digital graphic signature system of the present invention. The dialog may be used when someone other than the signatory, for example a merchant or notary, wishes to verify the signature. As set forth above, only a signatory may view the memo text associated with the signature. Further, although an optional comparison of the document and digital graphic signature held by the requesting party to that of a third party notary is not included in Figure 11, such features may be added by similar steps.

As shown in Figure 11, when a request for verification of a digital graphic signature is made by a third party requester, 171 the signatory's public key 154 is utilized to decode the document. This public key would have been previously supplied to the requester. The public key decrypts the document abstract 173. The decrypted abstract is compared to the actual document abstract, 175 and the results, or warnings in the case they do not match are displayed to the requester, 177.

Referring to Figure 11, the present invention advantageously provides a service through electronic mail, direct login, or the world wide web for electronic signature verification. In this case the verification requester sends the signed document, the document ID, and the signer's index to a signature guarantor. For example, on the world wide web, it may look like this:

http://www.citibank.com/verifysignature

Signature: (insert DigiGraphic signature)

of Signer: (insert Index)

Against: (insert Document ID)

With: (insert Abstract).

The index of the signer is unique to each signature guarantor, so they know who the signer is and what public key was used. Also, the document ID may be found in the wallet server, which archived at least the abstract of the document when the document was initially signed. Finally, the abstract is the document on which the verification requester is asking to have the signature verification performed.

The signature guarantor utilizes the index to look up the public key in the public key archive. The signature guarantor uses the public key, in turn, to decrypt the signature that is being verified. If the signature decrypts at all, then that verifies that the signature is from the signer of record. By using the document ID, the signature guarantor looks up its copy of the abstract, and compares it with the submitted abstract to further verify that it is the correct signature on the correct document. Then, the signature guarantor returns the results to the verification requester.

This feature of the present invention advantageously utilizes the index and document ID to verify the signature. On the other hand, current methods require certificates that contain very large amounts of information, such as the public key, the certifier of the certificate and the abstract. Further, because of this large amount of information, the signature guarantor using current methods has no active role in guaranteeing the process. On the other hand, the signature guarantor has a very active

role in the present invention. Thus, this feature of the present invention more efficiently and economically enables the verification of signatures.

As will be realized from the foregoing description, the digital graphic signature system of the present invention includes many advantageous features.

According to the present invention, a digital signature and a secret memo may advantageously be encoded into a single graphic signature.

An additional advantage is that the graphic signature is recognizable to the signer of the document who also has assurances that the signature is associated with a particular document and was actually signed by the signer and not forged.

A further advantage of the digital graphic signature system of the present invention is that the digital portion of the signature may be verified by a third party with knowledge of the public portion of the signatory's security key.

A still further advantage of the digital graphic signature system of the present invention is that the memo associated with a document remains secret to the signer of the document.

As in the description of a virtual wallet system of the present invention, the digital graphic signature system of the present invention may be advantageously utilized in conjunction with a virtual wallet system of the present invention.

Figure 12 provides a schematic representation of a digital graphic signature system of the present invention which includes a digital graphic signet. Encrypted abstract byte, 111 and encrypted memo byte, 113 are produced as described above and depicted in Figure 2. The off page connector "A" represents that stream entering the encoding process as it did before in the previous discussion. Likewise, The secret

memo is encoded in the same way as it was before. The off page connector "M" represents that stream entering the encoding process as it did before.

In the embodiment of a digital graphic signet of the present invention depicted in Figure 12, the red color byte value 302 is utilized for a private communication. As shown in Figure 12, a private communication, 304 may be reduced to textual representation and encrypted using the sender's (signatory) private key 306. The result of the encryption 308, is then encrypted again with the recipient's public key 310. The result of that last operation may then be used, byte for byte, as the red color value in the Color Point object stream described in the previous discussion with reference to Figure 2 on a digital graphic signature.

Upon receipt of the communication, the recipient will first use their private key to decrypt the first layer. Because they will be receiving a digital graphic signet with the document, which is distinct from a digital graphic signature, they will know that there is a private communication in the red color value and process it differently than they would a digital graphic signature. Once they have the first layer decrypted, they will use the public key of the sender to decrypt the final layer. Double encryption and the order of encryption and decryption is advantageous for several reasons.

If a single level encryption were used, if the sender used the public key of the recipient, then only the recipient could decode the message, which is one desirable trait. However, the recipient would not know for sure that the claimed sender was in fact the real sender without another digital signature.

Suppose that instead of using the recipient's public key, the sender uses their private key. Then the recipient can use the sender's public key to decrypt the message

and will know only they could have sent the message, the other desirable trait. This has a problem too, however, in that anyone else with knowledge of the sender's public key (which should be everyone since a public key is public) could also decrypt the message.

The usage of double encryption according to the present invention is novel and unique as it leverages off the concept of digital graphic signatures. The digital graphic signet may be a component of a document, and therefore may be flexible in how it is used.

For example, if the private communication is short, the content of the communication can be fully contained in the digital graphic signet. The abstract of the document would be used to convey the general nature, but not the details. The body of the document may be empty or a copy of the abstract.

In longer private communications, a symmetric key may be encoded in the digital graphic signet to be used to decode the body of the document. This is not unlike a "session key" described in conventional cryptographic literature. Another advantage of the digital graphic signet's flexibility is it can be used synchronously, as in an online session, or asynchronously, as in an E-mail document.

Although a digital graphic signet may be used in all transactions, it benefits may be found in communications other than those utilized to communicate actual online session keys, as there is already robust technology available (e.g. Diffie-Hellman), and that type of security is general at a lower level (transport layer vs. application layer) of network communications. A digital graphic signet could be used in addition to conventional session keys for added security. This is particularly

advantageous when the intent is to keep the content encrypted, and prevent it from appearing in the clear once it is received at the recipient's server.

For example, a bank customer may wish to change their ATM PIN over the Internet. The document could contain an abstract that might be as general as only indicating that it is a customer instruction to the bank. Since an ATM PIN change is a short message, the Signet would have the necessary account number, old PIN, and new PIN encoded into its red color value, as described earlier. Given an appropriate prevailing encryption technology is used, the strength of the encryption will be robust, the sender will be able to be authenticated, and only the intended recipient (the bank) will be able to see the details of the transaction. The abstract in the clear will give the bank processing center enough information to transport the Signet to an appropriately secure environment to decrypt and process the transaction without compromising the privacy or the security of the transaction.

Although the invention has been described with reference to preferred embodiments and features, other similar embodiments and features may be utilized to obtain similar results. Variations and modifications of the present invention will be apparent to one skilled in the art and the present disclosure is intended to cover all such modifications and equivalents within the scope of the following claims.

Claims:

1. A digital graphic signature for a transaction involving an individual the digital graphic signature having a visual representation comprising a plurality of points the digital graphic signature comprising:

merged points of at least a first color corresponding to transaction details data and points of at least a second color corresponding to the individual's signature data the points forming a visual representation of the individual's signature.

2. The digital graphic signature of claim 1 wherein the transaction details data comprise at least one of the following:

an abstract of the document being executed;

the body of the document being executed;

excerpts from the body of the document being executed; or

an individual's notes relating to the document being executed.

3. The digital graphic signature of claim 2 wherein the transaction details data comprise the abstract.

4. The digital graphic signature system of claim 3 wherein the abstract comprises a digest of what the individual is actually agreeing to by executing the document.

5. The digital graphic signature of claim 3 wherein the abstract comprises at least one of the following types of reference information: the date, the parties involved, or a transaction reference number.

6. The digital graphic signature of claim 3 wherein the abstract is in text.

7. The digital graphic signature of claim 2 wherein the transaction details data comprise excerpts from the body of the document being executed.

8. The digital graphic signature of claim 3 wherein the transaction details data comprise excerpts from the body of the document being executed.

9. The digital graphic signature of claim 7 wherein the excerpts are in text form.

10. The digital graphic signature of claim 2 wherein the transaction details data comprise the body of the document being executed.

11. The digital graphic signature of claim 2 wherein the transaction details data further comprise an individual's notes.

12. The digital graphic signature of claim 11 wherein the individual's notes comprise the purpose of the transaction, the nature of the transaction, or other details having significance to the individual.

13. The digital graphic signature of claim 3 wherein the transaction details data further comprises an individual's notes.

14. The digital graphic signature of claim 1 wherein the individual's signature data comprises graphical data generated from a graphic of the individual signature.

15. The digital graphic signature of claim 1 wherein the transaction details data and the individual's signature data are encrypted.

16. The digital graphic signature of claim 1 wherein the merged points are color encoded.

17. The digital graphic signature of claim 13 wherein the transaction details data
and the individual's signature data are color encoded wherein the abstract comprises blue values, the individual's notes comprise green values and the individual's signature data comprise red values.

18. The digital graphic signature of claim 1 wherein the visual representation is capable of being displayed on a video display terminal.

19. A digital graphic signature of claim 1 further comprising a digital graphic signet encoded in at least one of the plurality of colors.

20. A digital graphic signature system comprising:

the digital graphic signature of claim 1;

an input apparatus for the transaction details data;

an input apparatus for the signature data; and

a video display terminal.

21. A method for producing a digital graphic signature corresponding to a document executed by an individual, the method comprising:

forming an abstract of the document;

obtaining the individual's signature;

producing a document abstract data stream from the abstract;

producing a signature data stream from the signature; and

merging the document abstract data stream and the signature data stream into a digital graphic signature.

22. The method of claim 21 further comprising:

obtaining memo data from the individual;

producing a document memo data stream; and

merging the document abstract data stream, the document memo data stream and the signature data stream into a digital graphic signature.

23. A method for producing a digital graphic signature corresponding to a document executed by an individual, the document method comprising:

selecting details relating to the document;

forming an abstract of the document;

obtaining the individual's signature;

producing a document details data stream from the details;

producing a document abstract data stream from the abstract;

producing a signature data stream from the signature; and

merging the document details data stream; the document abstract data stream and the signature data stream into a digital graphic signature.

24. The method of claim 23 further comprising:

obtaining memo data from the individual;

producing a document memo data stream; and

merging the document details data stream; the document abstract data stream, the document memo data stream and the signature data stream into a digital graphic signature.

【図１】

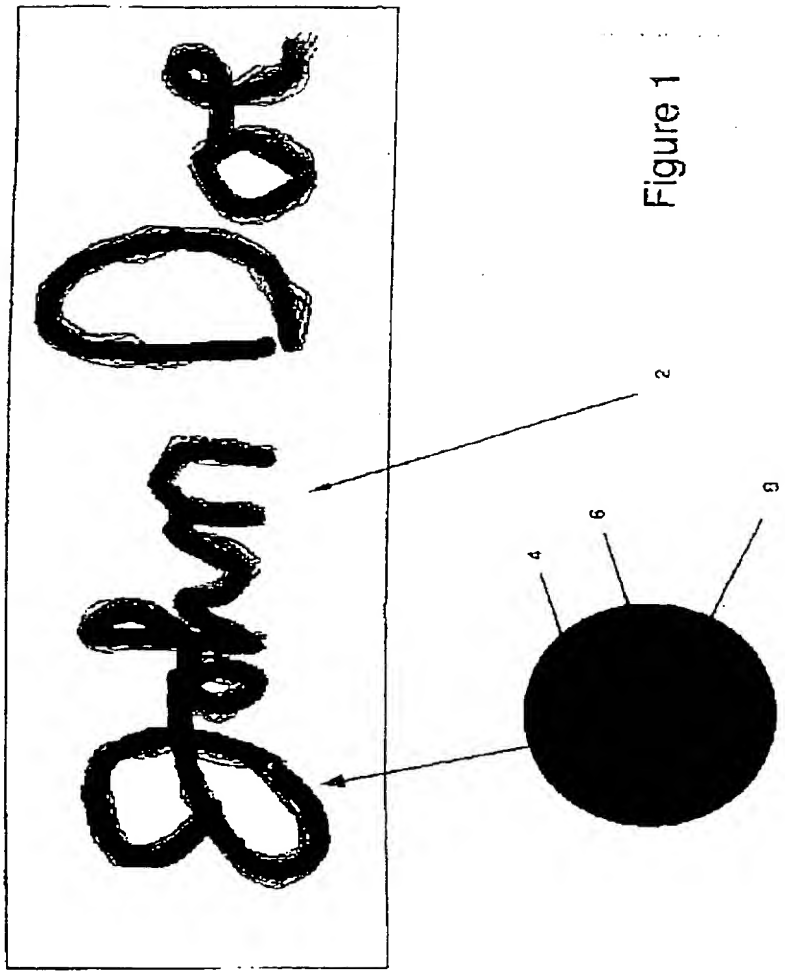
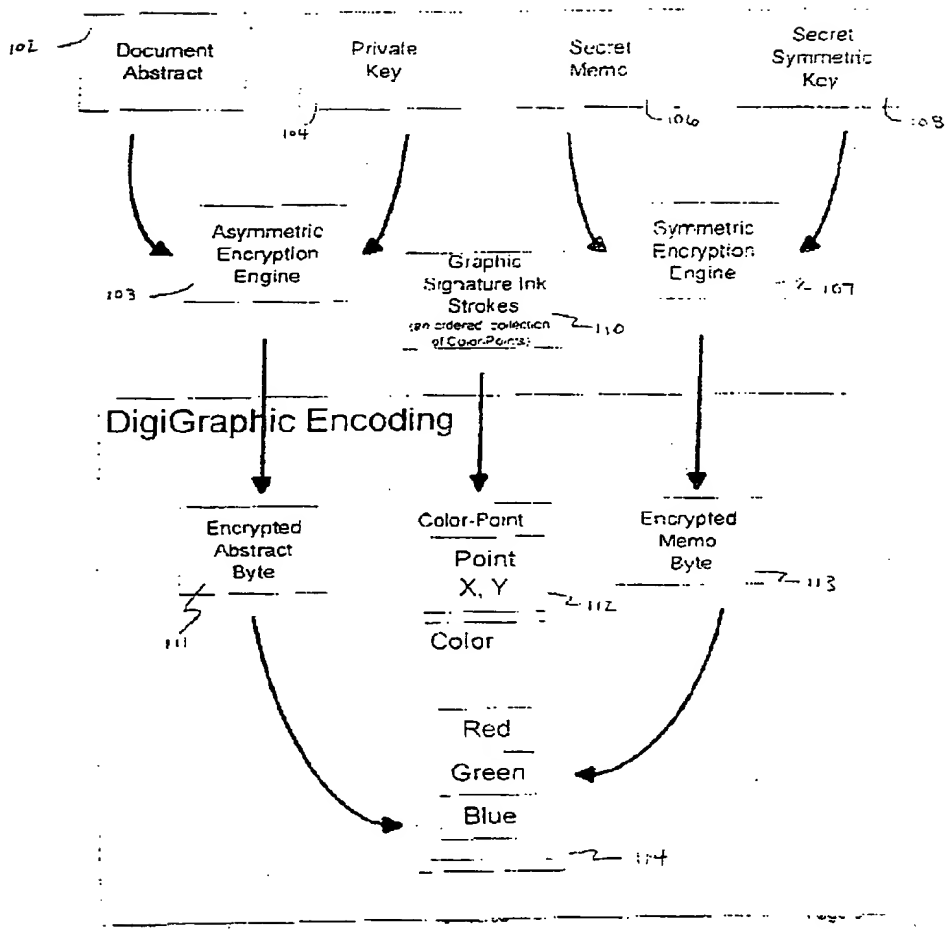


Figure 1

【図２】

FIGURE 2


101
Document Abstract
Private Key
104
Secret Memo
106
Secret Symmetric Key
108
Asymmetric Encryption Engine
103
Graphic Signature Ink Strokes
(an ordered collection of Color-Points)
110
Symmetric Encryption Engine
107
DigiGraphic Encoding
Encrypted Abstract Byte
111
Color-Point
Point X, Y
112
Color
Red
Green
Blue
114
Encrypted Memo Byte
113

【図３】

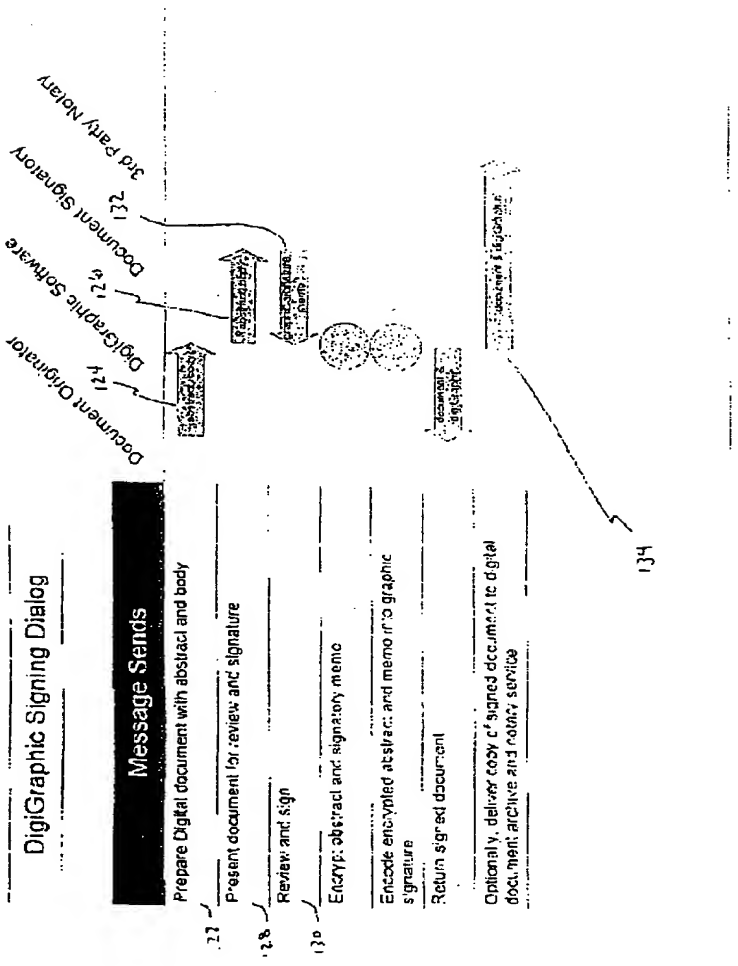

DigiGraphic Signing Dialog
Message Sends
Prepare Digital document with abstract and body
Present document for review and signature
Review and Sign
Encrypt abstract and signatory memo
Encode encrypted abstract and memo into graphic signature
Return signed document
Optionally, deliver copy of signed document to digital document archive and notary service
Document Originator
DigiGraphic Software
Document Signatory
3rd Party Notary
132
134

FIGURE 3

【図４】

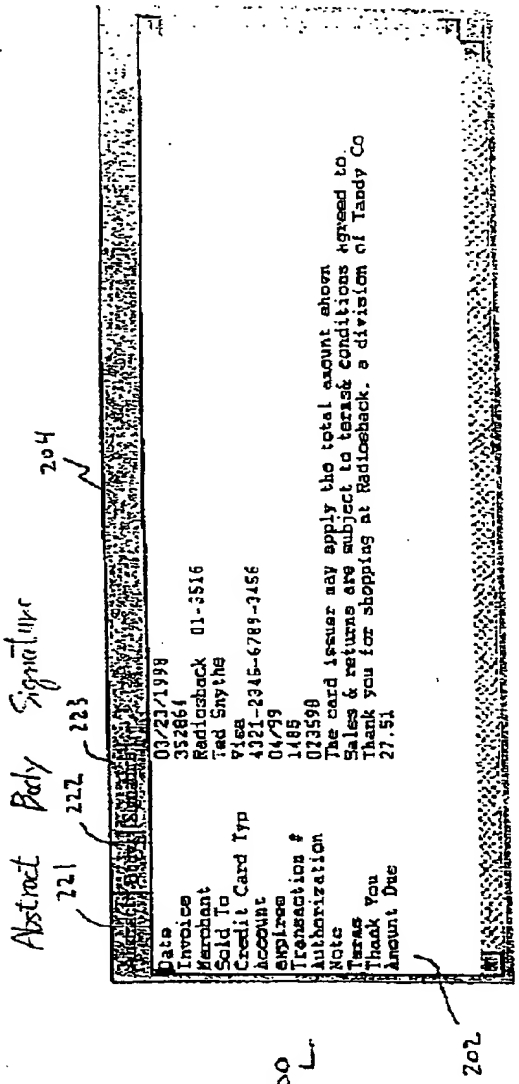

Abstract Body Signature
221
222
223
204
200
202
Date 03/23/1998
Invoice 352864
Merchant Radioshack 01-3516
Sold To Ted Smythe
Credit Card Typ Visa
Account 4321-2345-6789-3456
Expires 04/99
Transaction # 1485
Authorization 023598
Note The card issuer may apply the total amount shown
Terms Sales & returns are subject to terms& conditions agreed to
Thank You Thank you for shopping at Radioshack, a division of Tandy Co
Amount Due 27.51

FIGURE 4

【図５】

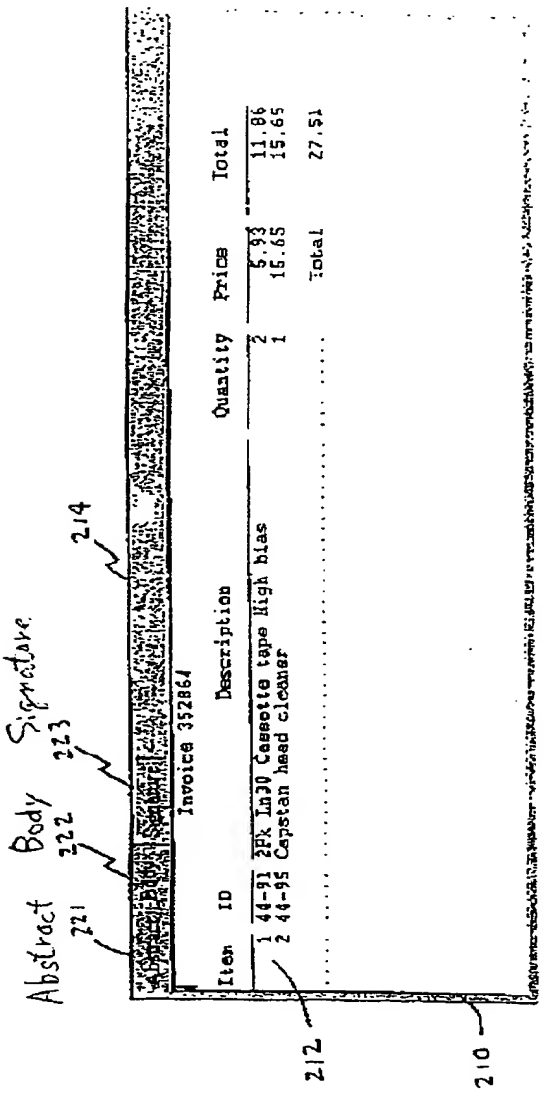

Abstract
221
Body
222
Signature
223
214
Invoice 352864
Item ID Description Quantity Price Total
1 44-91 2Pk In3D Cassette tape High bias 2 5.93 11.86
2 44-95 Capstan head cleaner 1 15.65 15.65
Total 27.51
212
210

FIGURE 5

【図６】

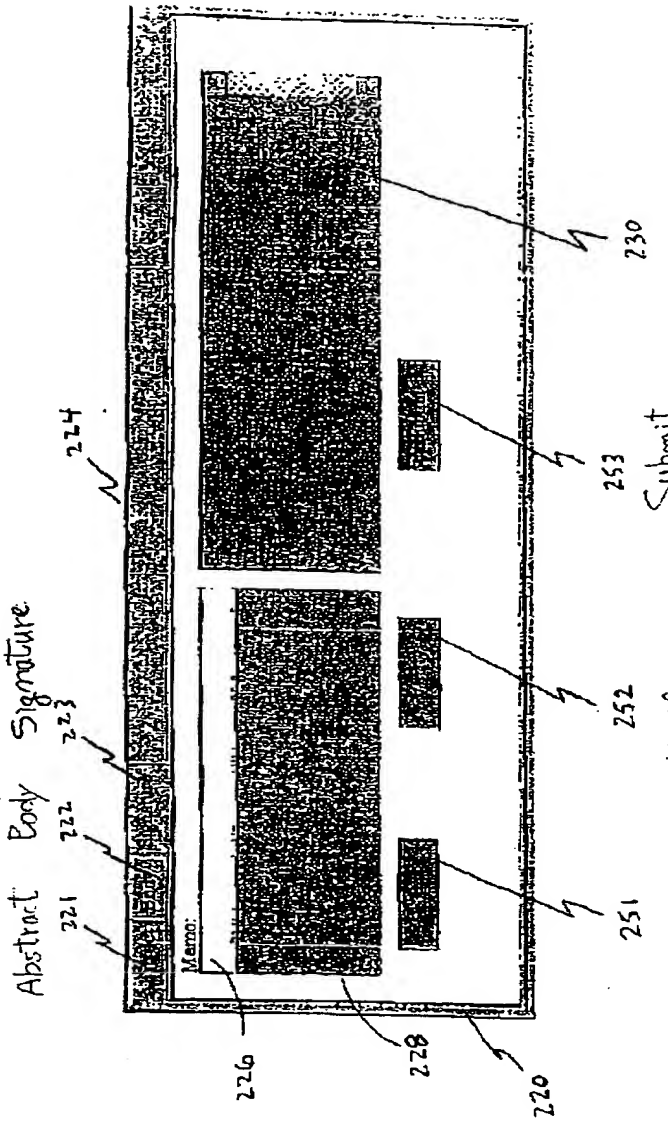

Abstract
Body
Signature
221
222
223
224
Memo:
226
228
220
251
252
253
230
Sign
Verify
Submit

FIGURE 6

【図７】

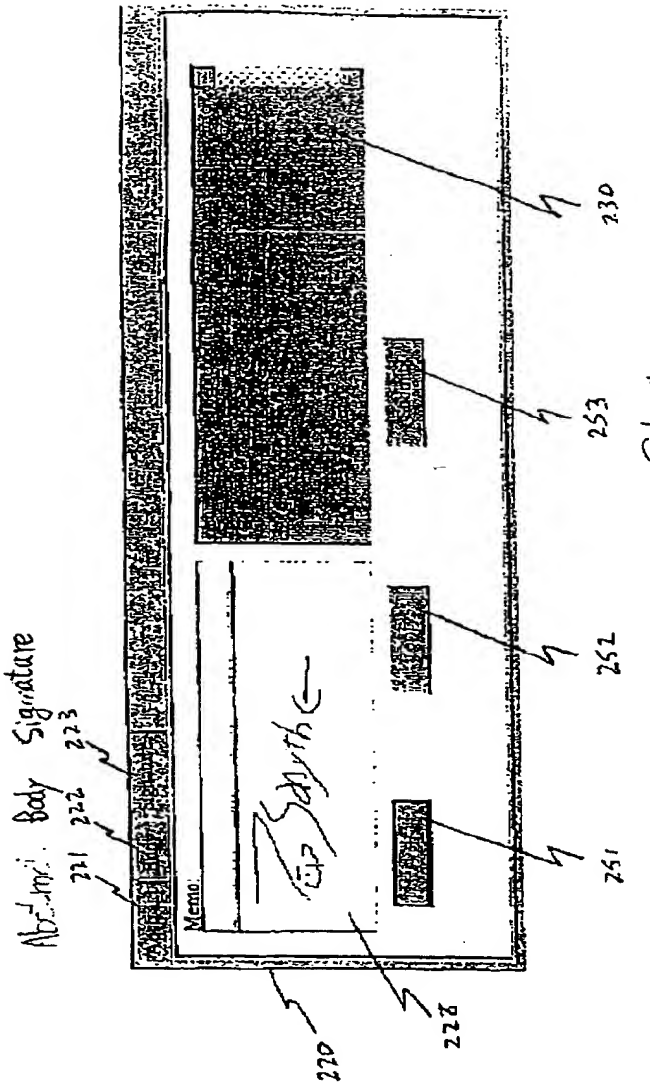

Author
Body
Signature
221
222
223
Memo
Sign
Verify
Submit
251
252
253
230
220
228

FIGURE 7

【図８】

Signatory Verification Dialog
Message Sends
Request signature verification with decryption of memo
Request verification of document to signature association
Decrypt memo using secret key
Decrypt abstract using public key
Compare document abstract to decrypted abstract
Display memo text
Display abstract text or mismatch warning message
150
153
155
157
159
161
Document Signatory
Digital Software
Digital Document
Digitographic Signature
152
154
151
Secret key
Public key

FIGURE 8

【図９】

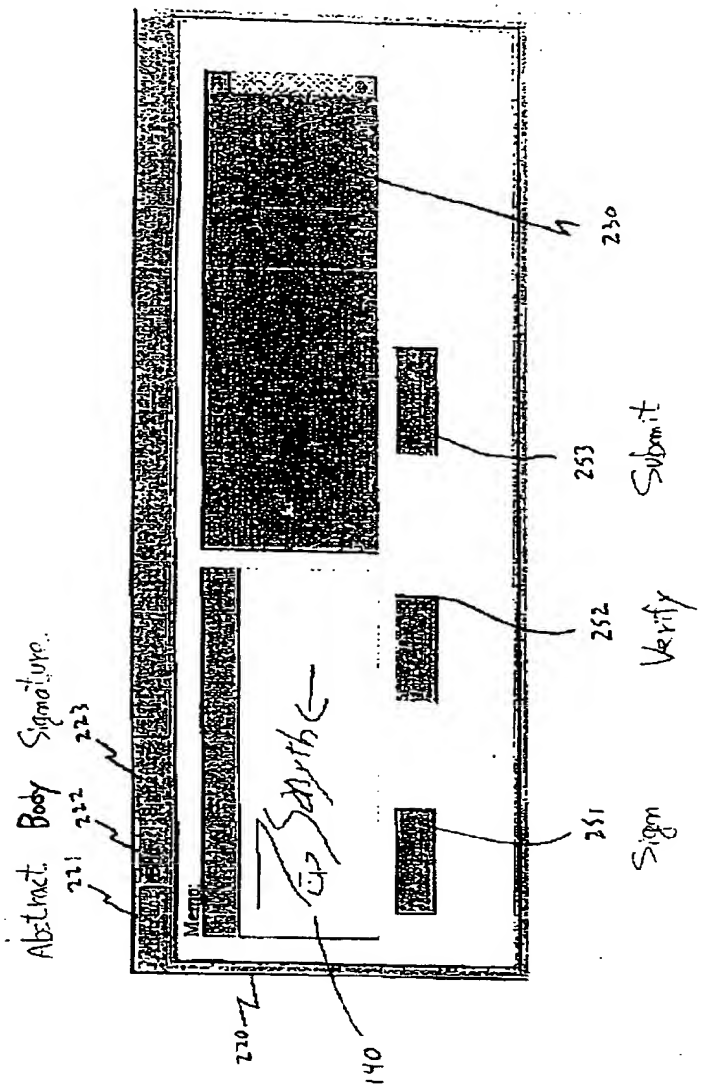

Abstract
Body
Signature
221
222
223
Memo
Tim Smyth
230
253
Submit
252
Verify
251
Sign
220
140

FIGURE 9

【図１０】

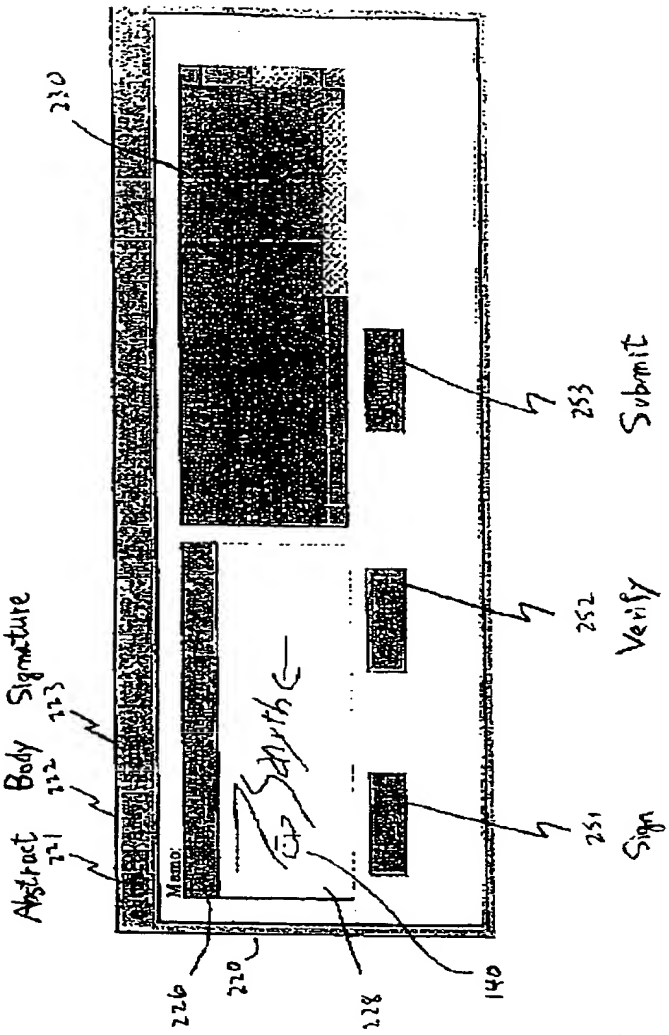


FIGURE 10

【図１１】

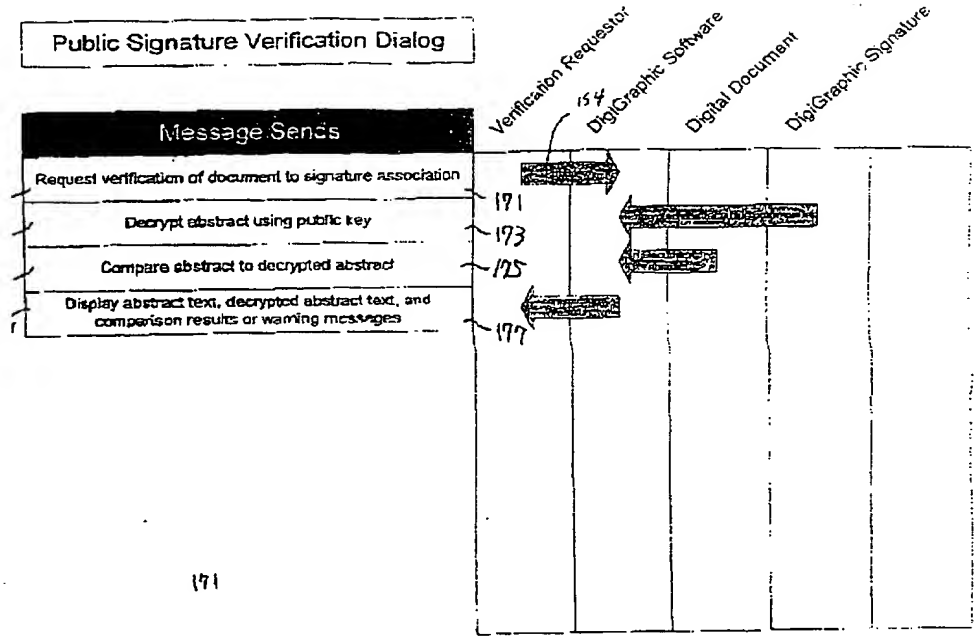


FIGURE 11

【図１２】

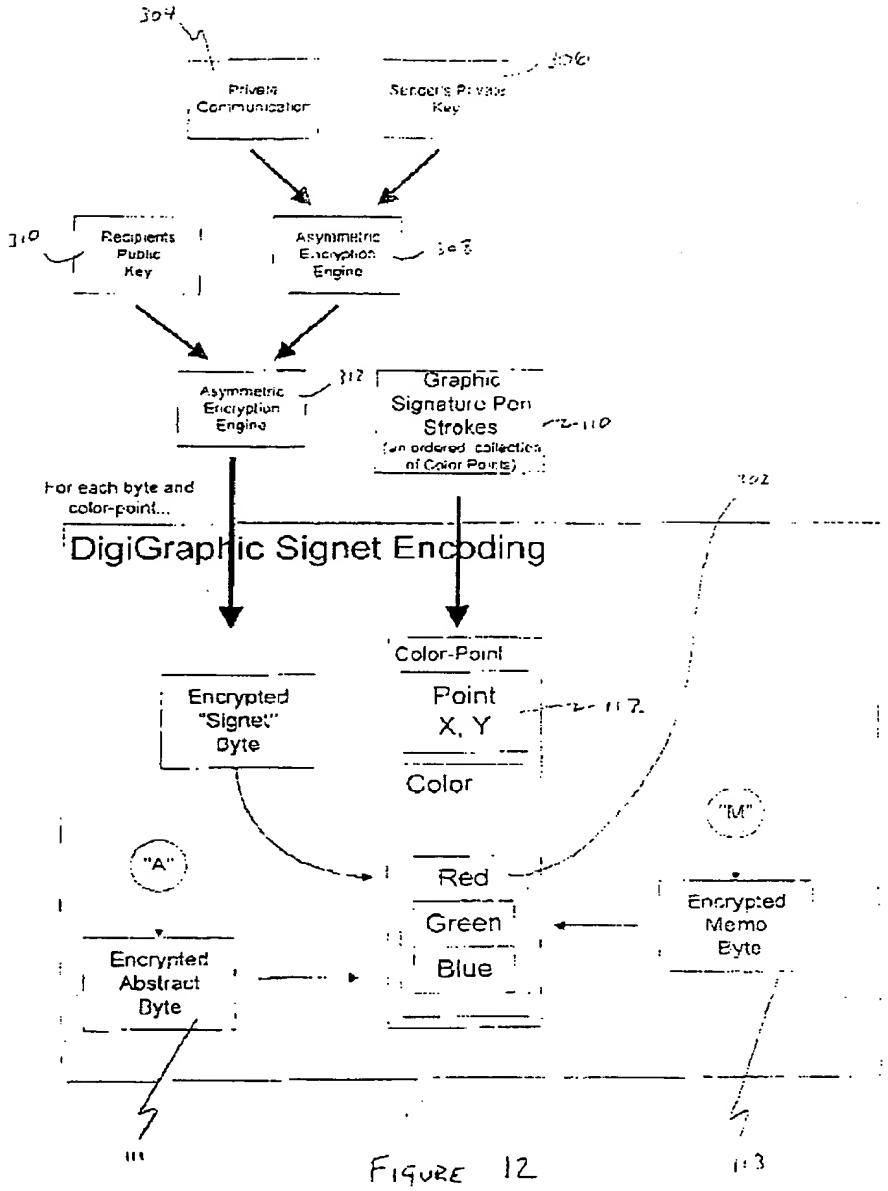


FIGURE 12

Abstract:

The present invention relates to a digital graphic signature system and methods for use in electronic commerce. The system comprises a document portion, including information relating to the document being executed, and a signature portion. The document portion and the signature portion may be encrypted and merged into a single object readily identifiable to an individual. The terminology "digital graphic signature" or "digigraphic signature" is utilized herein to describe the merged object.

The digital graphic signature system of the present invention may be advantageously utilized in electronic transactions, including transactions over the internet and network systems. The digital graphic signature system of the present invention may also be advantageously utilized in conjunction with information banking and virtual wallets.

Also disclosed is a digital graphic signet for transmitting a private communication.